
# E-Authentication Federation
# Interim Legal Document Suite

Version 4.0.7
10/14/05

## Release Notes

*Effective October 14, 2005.*

GSA

## Document History

| Status | Release | Date | Comment | Audience |
|---|---|---|---|---|
| Draft | 0.0.1 | 8/15/05 | Initial draft release. | Limited |
| Draft | 0.0.2 | 8/17/05 | • Added CSP Participating Agreement v2.1.0, Relying Party Participation Agreement v2.1.0, Business Rules v2.1.0, and Operating Rules v0.3.0.<br>• Made format changes.<br>• Made minor grammatical changes.<br>• Added Operating Rules to section 2.3 title.<br>• Placed operating rule footnotes into endnotes.<br>• Added Operating Rules to section 3.4.1.2 title.<br>• Replaced "Initiative" with "Federation" in section 4 title.<br>• Replaced "section 10" with "this section" in 4.10.1 and 4.10.4, | Limited |
| Draft | 3.0.0 | 8/25/05 | • Changed to version 3.0.0 to eliminate confusion on current version. | Limited |
| Draft | 3.0.1 | 8/30/05 | • Reference numbers 4.2.1, 4.4.3, 4.4.5, 4.6.4, 4.6.11, 4.7.1, 4.7.12, 4.7.18, 4.8.5, 4.8.10, 4.8.28, 4.8.31, 4.10.6, 4.10.8, 4.10.12, 4.14.3, 4.20.4, and 4.20.5. Modified section reference numbers as needed.<br>• Added new reference numbers 4.3.4, 4.3.13, 4.4.5, 4.5.1, 4.8.5, 4.12.6, 4.17.9, and 4.20.4. Modified section reference numbers as needed.<br>• Minor wording changes were made throughout the document.<br>• Added definition for compatible to Appendix A.<br>• Added S/MIME to Appendix B.<br>• Added text from 4.7.1 to 4.7.2 and changed "Primer" to "FAQ".<br>• Added two new bullets (numbers 1 and 5) to 4.8.11.<br>• Added a new bullet (number 2) to 4.8.25.<br>• Changed "EAI" to "EAI PMO" where appropriate. | Limited |
| Draft | 3.1.0 | 9/12/05 | • Added "logs as defined in these rules" to reference number 4.3.11.<br>• Added "appropriate" to reference number 4.3.13.<br>• Added "via means accessible only to Federation Members" to reference numbers 4.4.3 and 4.4.4.<br>• Changed "Federal PKI" to "Federation" and provided footnote pointing to Trust List to reference number 4.4.5.<br>• Added "subject to the terms of this agreement" to reference number 4.5.4.<br>• Added "based on the criteria in Appendix D" to reference number 4.5.9.<br>• Added "defined in section 4.10" to reference number 4.6.5.<br>• Added "and trusted" to reference number 4.17.13.<br>• Added "or subsequent revisions" to reference number 4.8.2.<br>• Added "or appropriately destroy" and "logs required by these rules " to reference number 4.8.9.<br>• Added "relevant" to reference number 4.8.10.<br>• Added "reasonable" and sentence "A list externally facing | Limited |

| Status | Release | Date | Comment | Audience |
|---|---|---|---|---|
| | | | systems…" to reference number 4.8.11.<br>• Added "or confidential" to reference number 4.8.17.<br>• Deleted "or suspected" from reference number 4.10.10 #1.<br>• Added "CSs may delay these new connections so that no more than three (3) new RP connections are established in any one 90 day period" to reference number 4.12.3.<br>• Added "Assertion-based RPs may delay these new connections so that no more than three (3) new CS connections are established in any one 90 day period" to reference number 4.12.4.<br>• Deleted reference numbers 4.12.6 and 4.20.4.<br>• Changed section 4.16 title to " Customer / Citizen Service".<br>• Added new definition for compatibility to Appendix A.<br>• Added SSA provided text to reference numbers 4.5.2 and 4.5.10.<br>• Changed Business Rules and Participation Agreements to reflect discussion of meetings held on August 29, 2005.<br>• Incorporated Fidelity and Treasury reactions to prior drafts of Business Rules and Participation Agreements. | |
| Draft | 3.2.0 | 9/13/05 | • Made changes to Appendix E.<br>• Added text for add-on services to reference numbers 4.14.2, 4.14.3, and 4.14.4. | Limited |
| Draft | 3.2.1 | 9/14/05 | • Removed Appendix E. | Limited |
| Draft | 3.2.2 | 9/19/05 | • Revised reference number 4.9.1 #2.<br>• Added Appendix E & F. | Limited |
| Draft | 3.2.3 | 9/26/05 | • Various typos removals, non-substantive wording clarifications, deletion of duplicative wording and format improvements were made throughout the Business Rules and Participation Agreements.<br>• Deleted reference to taxes and fees from Relying Party agreement, former section 2.8.10.<br>• Deleted reference to bankruptcy and assignment of rights to creditors from Relying Party agreement, section 2.8.11<br>• Deleted section 3.4, where the change control rules may have been housed. These rules are now an appendix of the Legal Suite.<br>• Second paragraph of section 1.2, further specifying role of DFA/CSP, was deleted.<br>• Sections 1.4 and 2.5 were deleted, in favor of consolidating all dispute resolution terms into a single section of each agreement.<br>• Section 1.4.1 and 2.5.1 were clarified to indicate all parties have orderly wind-down responsibilities.<br>• Sections 1.6.1 and 2.6.1 clarify that proposed changes in policy, practices or technology must be reported to GSA.<br>• Subsections within sections 1.5 and 2.6, addressing Dispute Resolution, were each consolidated.<br>• Sections 2.6.2 and 1.5.2 were amended to reference a | Limited |

| Status | Release | Date | Comment | Audience |
|---|---|---|---|---|
| | | | "reasonable determination" as opposed to the more relaxed standard of a "reasonable suspicion".<br>• Sections 1.6.2 and were clarified to indicated the liability limitation applies to circumstances related to the Agreement or to use of the Federation.<br>• Section 1.6.11 and 2.7.3 were clarified to indicate that surviving terms will be applicable whether the party has been terminated or suspended.<br>• Section 3.3.5.3 clarified to indicate only material non-compliance triggers need the provisions of this clause.<br>• Section 3.3.6.1 was clarified to indicate that the notice of emergency suspension or termination must be given to the other party that signed the Participation Agreement (e.g. a CSP must give notice to GSA and vice versa).<br>• Section 1.6.5, assignment, clarified point that a Treasury DFA can select agents and others to perform tasks.<br>• End-Notes were deleted from the Business Rules and Participation Agreements, as unnecessary, at request of commenters.<br>• Section 3.2.2 was clarified by deleting confusing language regarding conflicting terms of other agreements outside the Federation.<br>• All references to binding documents have been changed to the new section 3.3.3.2.<br>• 1.6.4 and 2.7.5 have been modified to delete the integration clause, because there are a number of other agreements at play between various of the parties.<br>• 3.3.5.5. – deleted wording that GSA reserves right to approve DFA, because the interagency agreement Draft already includes a process for collaborations. | |
| Draft | 3.2.4 | 09/28/05 | • Made acronym changes throughout the document.<br>• Removed references to the RPAF.<br>• Changed “AA” to “RP” in section 4.1.<br>• Added “the following rules apply” to each rule section in the operating rules.<br>• Provided new text for 4.2.1.<br>• Changed “numerous” to “particular” in section 4.3.<br>• Changed “EAI” to “Federation” in section 4.4.<br>• Provided text stating that RP and CSP reports are to be provided monthly.<br>• Changed text to say “active Federation Members in good standing” in 4.4.3 and 4.4.4.<br>• Changed “EST” to “ET” throughout document.<br>• Changed “seven (7) days per week” to “Monday through Friday” in 4.6.2.<br>• Changed “750 pixels by 80 pixels” to “140 pixels by 40 pixels” in 4.7.10.<br>• Replaced “RPAF” with “NIST SP 600-53” in 4.8.2.<br>• Changed “pass” to “participate in a suitable background evaluation” in 4.8.7. | Limited |

| Status | Release | Date | Comment | Audience |
|---|---|---|---|---|
| | | | • Changed text in reference number 4.8.9 specifying confidential information from the EAI PMO.<br>• Added "intrusive testing" to 4.8.11, number 3.<br>• Added "and confidential" to 4.8.16.<br>• Changed text in 4.8.18 specifying when outside the firewall and attempting to access a Federation system root.<br>• Changed "should" to "must", added "and unused", and added the sentence "It is recommended that unneeded services be removed".<br>• Removed session management section.<br>• Removed bullet one and change bullet five text stating "unauthorized changes" in section 4.10 (now 4.9).<br>• Added "publish" to 4.11.5 (now 4.10.5).<br>• Changed text in 4.12.1 (now 4.11.1) to "substantial changes that affect other Federation Member systems".<br>• Changed "one" to "given" in 4.12.4 (now 4.11.4) and 4.12.5 (now 4.11.5).<br>• Deleted "if they are restricted under privacy regulations, policy, and law" from 4.13.1 (now 4.12.1)<br>• Changed section 4.16 (now 4.15) to "End-User Service".<br>• Added "as amended from time-to-time" to section 4.20 (now 4.19).<br>• Provided new text for section 4.21 (now 4.20).<br>• Removed DRAFT watermark. | |
| Release | 4.0.0 | 09/29/05 | Official document release. | Public |
| Release | 4.0.1 | 10/03/05 | Deleted section 4.1.2 and added text for the TBDs in Appendix F. | Public |
| Revision | 4.0.2 | 10/10/05 | • Made sentence wording changes throughout the document.<br>• Changed section reference to 1.6.11 in section 1.4.<br>• Changed section reference to 3.3.6.6 in section 3.2.2.<br>• Added an additional sentence to the end of section 3.3.5.5.<br>• Deleted "This document is a normative specification" from section 4.1.1.<br>• Changed section reference to 1.6.8 in section 4.7.<br>• Deleted reference numbers 4.8.17 and 4.8.22.<br>• Changes section 4.19 title to "Authoritative Documents".<br>• Added text from section 1.7 to section 2.8. | Limited |
| Revision | 4.0.3 | 10/11/05 | • Added "Interim" to title of document.<br>• Added "Interim" to section 3 title.<br>• Removed reference to suspension policy.<br>• Made additional sentence wording changes. | Limited |
| Revision | 4.0.4 | 10/13/05 | • Capitalized all defined terms throughout the document.<br>• Capitalized "section" throughout the document.<br>• Added 3rd party to section 1.6.5.<br>• Added new text for section 1.6.7 and 1.6.8.<br>• Changed date to October 31, 2006 in section 1.6.15.<br>• Added new sub-sections from CSP Agreement to section 2. | Limited |

| Status | Release | Date | Comment | Audience |
|---|---|---|---|---|
| | | | • Added new text to section 2.7.2.<br>• Deleted section 2.7.7.<br>• Changed date to October 31, 2006 in section 2.7.12.<br>• Changed reference to 3.3.6.2 in section 3.3.3.4.2.<br>• Added sentence for scope of auditing in section 3.3.5.2.<br>• Deleted section 3.3.6.4.<br>• Revised text in section 3.3.6.6.<br>• Deleted reference number 4.8.9.<br>• Replaced "certified" with "approved" throughout the document.<br>• Revised definition of Relying Party.<br>• Added definitions for Business Rules, Agency, Boarding Process, Binding Documents, Contractor, Operational Readiness Review, Designated Financial Agent, and Sensitive Information.<br>• Added updated governance diagram to Appendix E.<br>• Changed the effective date to October 14, 2005. | |
| Revision | 4.0.5 | 10/13/05 | • Added definition for "The Approved Technology Provider List".<br>• Replaced "EAI PMO" with "GSA".<br>• Removed definition for "Certified Credential Service".<br>• Provided new definition for "Availability".<br>• Removed "RPAF" from the acronym list.<br>• Changed "certify" to "approve".<br>• Made minor sentence mortifications throughout the document. | Limited |
| Revision | 4.0.6 | 10/14/05 | • Removed EAI from section 4.<br>• Changed title of section 4.12 to "Optional Attributes".<br>• Revised 1st paragraph and added new paragraph for CSPs in section 3.3.1.<br>• Revised 1st sentence in section 3.3.3.3.<br>• Replaced "through" with "in conjunction with" in section 3.3.6.5. | Limited |
| Revision | 4.0.7 | 10/14/05 | • Added new sentence to section 3.3.1. | Limited |

## Editors

| | | |
|---|---|---|
| Chris Louden | Dave Silver | J.T. Lazo |
| Chris Broberg | David Simonetti | Steve Lazerowich |
| Glenn Ballard | Andrew Chiu | Dan Greenwood |

# Table of Contents

# 1 E-AUTHENTICATION FEDERATION CSP PARTICIPATION AGREEMENT

## 1.1 Scope and Application

This Participation Agreement constitutes the legal basis for an organization becoming a Credential Service Provider (CSP) within the E-Authentication Federation. Signatories agree that the signed Participation Agreement, Business Rules, and Operating Rules, including the Binding Documents referenced in Section 3.3.3.2 of the Business Rules, govern participation in the E-Authentication Federation. Final approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. Such GSA approval is contingent upon the CSP successfully completing the Boarding Process and Operational Readiness Review. Signatories agree to abide by all applicable laws and regulations, including those relating to privacy, and record keeping.

## 1.2 Parties and Contact Person

The parties to this Participation Agreement are the General Services Administration of the United States Federal Government (GSA) and _____ (CSP). Each party shall designate one or more contact persons for purposes of notices and other communications under the Business Rules, Operating Rules and this Participation Agreement.

## 1.3 Agreement to Abide by Business Rules and Operating Rules

By signing this Participation Agreement, the CSP agrees to abide by the E-Authentication Federation Business Rules and Operating Rules as in effect during the period of CSP participation in the E-Authentication Federation, and which are expressly incorporated into and made a part of this Agreement.

## 1.4 Compliance With Requirements

CSP agrees that compliance with the Credential Assessment Framework (CAF), including security requirements specified in the Operating Rules, is a prerequisite to participation in the E-Authentication Federation and must be finalized before approval for inclusion in the E-Authentication Federation. CSP agrees to maintain continuing compliance with CAF and other terms contained in the Business Rules and Operating Rules.

## 1.5 Termination and Suspension

The terms of this Participation Agreement cease to apply to any CSP as of the effective date of termination of participation in the E-Authentication Federation, except surviving terms, according to Section 1.7.11.

### *1.5.1 Voluntary*

This CSP Participation Agreement may be terminated at the discretion of the CSP, upon written notice to GSA or by mutual agreement between GSA and the CSP, reflected in a signed writing, provided that in the event of any such voluntary termination each party remains responsible to the extent practicable for an orderly wind down of activities or services in progress and for the maintenance of the records of such activities and services.

### *1.5.2 Involuntary*

GSA may terminate or suspend the participation of a CSP in the E-Authentication Federation, at any time, under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation, or for breach by the CSP of the terms of this Participation Agreement, the Business Rules or the Operating Rules, that the CSP is unable to cure within 30 days after receiving notice from GSA regarding such breach. Termination shall be in writing and shall be effective no less than 30 days from time notice is given, unless a shorter period or immediate termination is required in the reasonable judgement of GSA. Suspension may occur at any time, as the needs and circumstances may reasonably require, with notice to the CSP as soon as practicable.

## 1.6 Enforcement

CSP and GSA agree that the following provisions are related to enforcement, recognizing that such provisions are incorporated into the Participation Agreements executed by all Approved Parties.

### *1.6.1 Dispute Resolution*

Every Approved Party or its authorized agent agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of the Business Rules, the Operating Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. In the event the parties are unable to resolve the matter, then each such dispute, the date of attempted resolutions, including proposed changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA to investigate the dispute and may propose resolution or mediate at the request of the parties. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

### *1.6.2 GSA Investigation*

GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

GSA may initiate an investigation based upon the request of any Approved Party in the E-Authentication Federation, or may initiate an investigation whenever it deems appropriate based on any information it regards as relevant and credible. Without

limitation, such information may include a reasonable determination that an Approved Party is not in compliance with continuing obligations required under this Participation Agreement, the Business Rules or the Operating Rules. An Approved Party shall be notified in a timely manner by GSA if it becomes the subject of an investigation.

### *1.6.3 Recourse*

Based upon the results of its investigation, and only under extraordinary circumstances necessary to prevent or limit serious harm to the E-Authentication Federation, the GSA may suspend participation of any Approved Party in the E-Authentication Federation or render inaccessible any Architectural Component of the E-Authentication Federation by one or more Approved Parties. An Approved Party has the right to appeal any proposed suspension, including being provided adequate notice and an opportunity to be heard. If the result of an investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules or the Operating Rules, GSA may require such additional audit, re-approval or approval at different Level(s) of Assurance, to the extent necessary to prevent or limit serious harm to the E-Authentication Federation.

## 1.7 Legal Terms

### *1.7.1 Confidentiality and Non-Disclosure*

GSA agrees not to unreasonably withhold assent to industry standard confidentiality and/or non-disclosure agreements with the CSP that may be required as a condition of accepting Approved Credentials of that CSP and according to the Business Rules and Operating Rules. GSA further agrees to require consent to the relevant terms of such agreements by any Relying Party to whom the terms may apply.

### *1.7.2 Limitation of Liability*

Liability against the United States for damage caused by negligence of the Government is controlled by the Federal Tort Claims Act, 28 USC Section 1346 et seq. A non-governmental Approved CSP operating in accordance with the terms of this CSP Participation Agreement, the Business Rules and the Operating Rules, may assert the Government contractor defense to tort claims arising out of or related to participation in the E-Authentication Federation.

There shall be no liability against any Approved Party under any theory of liability for any claim arising out of or in relation to this Agreement or to the use of or reliance upon an Approved Credential or participation in the E-Authentication Federation, beyond the recourse available under the Federal Tort Claims Act, unless agreed by contract among the relevant parties.

### *1.7.3 Governing Law*

This Participation Agreement, the Business Rules and the Operating Rules and any related materials governing the E-Authentication Federation shall be construed and

adjudicated according to the statutes, regulations and judicial decisions of the United States of America.

### *1.7.4 Order of Precedence*

The parties agree to interpret the provisions of all E-Authentication documents to be consistent, to the maximum extent reasonable and practicable. However, in the event of a conflict between the terms of various E-Authentication Federation related documents, documents shall be accorded the following order of priority: This CSP Participation Agreement shall be construed to prevail over the terms of any other document in the E-Authentication Legal Suite, followed in order of precedence by the terms of the E-Authentication Federation Business Rules, followed by the terms of the Operating Rules, followed by the terms of any Binding Document referenced in Section 3.3.3.2 of the Business Rules, followed by any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

### *1.7.5 Assignment, Succession and Bankruptcy*

CSP agrees it may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this CSP Participation Agreement, the E-Authentication Federation Business Rules or the Operating Rules except as permitted herein. CSP may request of GSA permission for assignment or succession to a different party, of part or all of the rights and/or obligations contained in this CSP Participation Agreement, the E-Authentication Federation Business Rules or the Operating Rules. Nothing in this paragraph shall be construed as to prevent the Department of the Treasury from Designating Financial Agents to carry out its obligations under this agreement, in accord with the terms of Section 3.3.5.5 of the Business Rules, or to prohibit such agents from the use of contractors, affiliates or other third parties. Any prohibited assignment shall be null and void.

CSP or an agent thereof may engage its affiliates and/or third parties to perform certain of its obligations contained in this CSP Participation Agreement, the E-Authentication Federation Business Rules or the Operating Rules. For purposes of this Agreement, Affiliate shall mean any entity directly or indirectly Controlling, Controlled by or under common Control with a CSP. For purposes of this provision, Control means an ownership interest of 50 percent or more.

### *1.7.6 Severability*

If any provision, set of provisions or part of a provision of this Participation Agreement, the Business Rules or the Operating Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

### 1.7.7 Grant of License

For the term of this Participation Agreement, CSP is hereby granted a perpetual, non-exclusive, royalty free, non-transferable license to use the Architectural Component known as the Portal required for participation in the E-Authentication Federation, including the right to access and grant access to other authorized parties to such components and to Systems and applications of Approved Relying Parties.

### 1.7.8 Ownership of Intellectual Property

Ownership and control of all databases, records, and data transmission systems remains solely with the CSP. CSP hereby grants all Approved Parties of the E-Authentication Federation a perpetual, royalty-free, non-exclusive, non-transferable license to use any methods or other intellectual property of the CSP solely for use within the E-Authentication Federation and in accordance with the E-Authentication Federation Business Rules and Operating Rules (the "Approved Purpose"). Such license includes the right to practice, solely for the Approved purpose, under claims in any United States patent granted to CSP and its affiliates. Usage of this license by any Approved Parties will require a reciprocal, perpetual, royalty-free non-exclusive, non-transferable license to CSP from any other Approved Parties in connection with CSP's participation.

### 1.7.9 Publicity

No Signatory may make any public claims regarding any other Signatory without that party's prior written approval, including use of the name of a CSP by GSA or a Relying Party or any suggestion of endorsement of a CSP by GSA or any Relying Party. The foregoing limitation shall not apply to use of the name of a CSP on the Trusted Credential Service Provider List or in any other way authorized under these Business Rules or Operating Rules and other Binding Documents referenced in Section 3.3.3.2.

### 1.7.10 Waiver

Neither party's failure to enforce strict performance of any provision of this Participation Agreement, the Business Rules or the Operating Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of this Participation Agreement, the Business Rules or the Operating Rules.

### 1.7.11 Survival

Any termination or suspension of CSP's participation in the E-Authentication Federation shall not affect any accrued rights or liabilities of any party nor shall it affect the coming into force or the continuance in force of any provision of this Participation Agreement which is expressly or by implication intended to come into force or continue in force on or after such termination or suspension.

### *1.7.12 Amendment*

This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

### *1.7.13 Responsibility For Taxes, Expenses*

Each party agrees that each are solely responsible for the payment of taxes or expenses incurred by that party arising out of or related to participation in the E-Authentication Federation, unless otherwise agreed by a signed writing.

### *1.7.14 Force Majeure*

Neither party shall be considered in default hereunder due to any failure in performance of its obligations under this Participation Agreement, the Business Rules or the Operating Rules, including any Binding Document referenced in Section 3.3.3.2, should such failure arise out of causes beyond its reasonable control and without its fault or negligence.

### *1.7.15 Business Rules and Operating Rules Freeze*

The parties agree that, unless otherwise agreed to in writing, the Business Rules or the Operating Rules are not intended to be, and shall not be amended for a period of one year from the date of execution of this Participation Agreement or before October 31, 2006, whichever date shall precede the other.

## 1.8 Signatures

The undersigned represent and warrant that they have the requisite power and authority to execute this Participation Agreement on behalf of their respective organizations (the Parties), including authority to legally bind their respective organizations to the Binding Documents referenced in Section 3.3.3.2 of the Business Rules.

| | |
|---|---|
| _____ | _____ |
| CSP | GSA |

# 2 E-AUTHENTICATION FEDERATION RELYING PARTY PARTICIPATION AGREEMENT

## 2.1 Scope and Application

This Relying Party Participation Agreement constitutes the legal basis for an organization becoming a Relying Party within the E-Authentication Federation. Signatories agree that the signed Participation Agreement, Business Rules and the Operating Rules, including the Binding Documents referenced in Section 3.3.3.2 of the Business Rules, govern participation in the E-Authentication Federation. Final approval by the GSA is necessary for a Relying Party to participate in the E-Authentication Federation. Such GSA approval is contingent upon the Relying Party successfully completing the Boarding Process and Operational Readiness Review. Signatories agree to abide by all applicable laws and regulations, including those relating to privacy, and record keeping.

## 2.2 Parties and Contact Person

The parties to this Participation Agreement are the General Services Administration of the United States Federal Government (GSA) and _____ (Relying Party). Each party shall designate one or more contact persons for purposes of notices and other communications under the Business Rules, Operating Rules and this Participation Agreement.

## 2.3 Agreement to Abide by Business Rules and Operating Rules

By signing this Participation Agreement, the Relying Party agrees to abide by the E-Authentication Federation Business Rules and Operating Rules, as in effect during the period of participation in the E-Authentication Federation, and which are expressly incorporated into and made a part of this Agreement.

## 2.4 Compliance With Requirements

Relying Party agrees that compliance with NIST SP 800-53 and the security requirements specified in the Operating Rules, are prerequisites to participation in the E-Authentication Federation and must be finalized before approval for inclusion in the E-Authentication Federation. Relying Party agrees to maintain continuing compliance with NIST SP 800-53 and other terms contained in the Business Rules and Operating Rules.

## 2.5 Termination and Suspension

The terms of this Participation Agreement, the Business Rules and the Operating Rules cease to apply to any Relying Party as of the effective date of termination of participation in the E-Authentication Federation except for the surviving terms, according to Section 2.7.4.

### *2.5.1 Voluntary*

Participation in the E-Authentication Federation may be terminated by Relying Party through written notice to GSA, to avoid the imminent effect of amended language to the Business Rules or Operating Rules. Such termination shall be effective no less than 30 calendar days from the date of receipt by GSA. Relying Party may terminate its participation in the E-Authentication Federation, without cause, upon 60 days prior written notice to GSA. In the event of extraordinary emergency circumstances for which relief is not possible in the context of continued participation, a Relying Party may terminate participation immediately, provided that both parties remains responsible to the extent practicable for an orderly wind down of activities or services in progress and for the maintenance of the records of such activities and services. Participation in the E-Authentication Federation may also be terminated at any time for any reason by mutual agreement between the GSA and Relying Party.

### *2.5.2 Involuntary*

GSA may suspend the participation of any Relying Party in the E-Authentication Federation, and only under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation.

## 2.6 Enforcement

Relying Party and GSA agree that the following provisions are related to enforcement, recognizing that such provisions are incorporated into the Participation Agreements executed by all Approved Parties.

### *2.6.1 Dispute Resolution*

Every Approved Party agrees to attempt in a timely manner to resolve any dispute arising out of or related to the application of the Business Rules, the Operating Rules or the Participation Agreement executed by that Approved Party in good faith with the other disputants and parties related to the dispute. In the event the parties are unable to resolve the matter, then each such dispute, the date of attempted resolutions, including proposed changes in policy, practices or technology implementation, shall be reported to the GSA in a timely manner.

In the event parties to a dispute are unable, despite their best good faith efforts, to resolve a dispute among themselves, any party may request GSA to investigate the dispute and may propose resolution or mediate at the request of the parties. Each such request must be accompanied by a full report of all the relevant information related to the dispute.

### *2.6.2 GSA Investigation*

GSA shall respond to every request to investigate a dispute in a timely manner. GSA may request additional information from one or more parties to the dispute.

GSA may initiate an investigation based upon the request of any Approved Party in the E-Authentication Federation, or may initiate an investigation whenever it deems

appropriate based on any information it regards as relevant and credible. Without limitation, such information may include a reasonable determination that an Approved Party is not in compliance with continuing obligations required under this Participation Agreement, the Business Rules or the Operating Rules. An Approved Party shall be notified in a timely manner by GSA if it becomes the subject of an investigation.

### *2.6.3 Recourse*

Based upon the results of its investigation, and only under extraordinary circumstances necessary to prevent or limit serious harm to the E-Authentication Federation, the GSA may suspend participation of any Approved Party in the E-Authentication Federation or render inaccessible any Architectural Component of the E-Authentication Federation by one or more Approved Parties. An Approved Party has the right to appeal any proposed suspension, including being provided adequate notice and an opportunity to be heard. If the result of an investigation indicates that an Approved Party is not in compliance with any requirement included directly or by reference under these Business Rules or the Operating Rules, GSA may require such additional audit, re-approval or approval at different Level(s) of Assurance, to the extent necessary to prevent or limit serious harm to the E-Authentication Federation.

## 2.7 Legal Terms

### *2.7.1 Governing Law*

This Participation Agreement, the Business Rules and the Operating Rules and any related materials governing the E-Authentication Federation shall be construed and adjudicated according to the statutes, regulations and judicial decisions of the United States of America.

### *2.7.2 Grant of License*

For the term of this Participation Agreement, Relying Party is hereby granted a perpetual, non-exclusive, royalty free, non-transferable license to use the Architectural Component known as the Portal required for participation in the E-Authentication Federation, including the right to access and grant access to other authorized parties to such components and to Systems and applications of Approved Relying Parties.

### *2.7.3 Ownership of Intellectual Property*

Ownership and control of all databases, records, and data transmission systems remains solely with the Relying Party. Relying Party hereby grants all Approved Parties of the E-Authentication Federation a perpetual, royalty-free, non-exclusive, non-transferable license to use any methods or other intellectual property of the Relying Party solely for use within the E-Authentication Federation and in accordance with the E-Authentication Federation Business Rules and Operating Rules (the “Approved Purpose”). Such license includes the right to practice, solely for the Approved purpose, under claims in any United States patent granted to the Relying Party and its affiliates. Usage of this license by any Approved Parties will require a reciprocal, perpetual, royalty-free non-exclusive,

non-transferable license to the Relying Party from any other Approved Parties in connection with Relying Party's participation.

### 2.7.4 Survival

Any termination or suspension of Relying Party's participation in the E-Authentication Federation shall not affect any accrued rights or liabilities of either party nor shall it affect the coming into force or the continuance in force of any provision of this Participation Agreement which is expressly or by implication intended to come into force or continue in force on or after such termination or suspension.

### 2.7.5 Confidentiality and Non-Disclosure

Relying Party agrees not to unreasonably withhold assent to industry standard confidentiality and/or non-disclosure agreements participating CSPs may require as a condition of accepting Credentials of that CSP and according to the Business Rules and Operating Rules.

### 2.7.6 Order of Precedence

The parties agree to interpret the provisions of all E-Authentication documents to be consistent, to the maximum extent reasonable and practicable. However, in the event of a conflict between the terms of various E-Authentication Federation related documents, documents shall be accorded the following order of priority: This Relying Party Participation Agreement shall be construed to prevail over the terms of any other document in the E-Authentication Legal Suite, followed in order of precedence by the terms of the E-Authentication Federation Business Rules, followed by the terms of the Operating Rules, followed by the terms of any Binding Document referenced in Section 3.3.3.2 of the Business Rules, followed by any other policies, agreements or other materials formally promulgated for the purpose of documenting legal terms governing participation in the E-Authentication Federation.

### 2.7.7 Severability

If any provision, set of provisions or part of a provision of this Participation Agreement, the Business Rules or the Operating Rules is held to be unenforceable or otherwise invalid in whole or in part, the remaining provisions shall remain in full force and effect and shall be construed to the maximum extent practicable as a consistent and reasonable entire agreement.

### 2.7.8 Amendment

This Participation Agreement may be amended by agreement of the parties, reflected by a signed writing.

### *2.7.9 Publicity*

No Signatory may make any public claims regarding any other Signatory without that party's prior written approval, including use of the name of a Relying Party by GSA or a CSP or any suggestion of endorsement of a Relying Party by GSA or any CSP. The foregoing limitation shall not apply to use of the name of a Relying Party in any other way authorized under these Business Rules or Operating Rules and other Binding Documents referenced in Section 3.3.3.2.

### *2.7.10 Waiver*

Neither party's failure to enforce strict performance of any provision of this Participation Agreement, the Business Rules or the Operating Rules will constitute a waiver of a right to subsequently enforce such a provision. No written waiver shall constitute, or be construed as, a waiver of any other obligation or condition of this Participation Agreement, the Business Rules or the Operating Rules.

### *2.7.11 Force Majeure*

Neither party shall be considered in default hereunder due to any failure in performance of its obligations under this Participation Agreement, the Business Rules or the Operating Rules, including any Binding Document referenced in Section 3.3.3.2 should such failure arise out of causes beyond its reasonable control and without its fault or negligence.

### *2.7.12 Assignment and Succession*

Relying Party may not sell, rent, lease, sublicense, assign, grant a security interest in or otherwise transfer any right and/or obligation contained in this Participation Agreement, the Business Rules or the Operating Rules, except as permitted herein. Relying Party may request of GSA permission, which permission shall not be unreasonably withheld, for assignment or succession to a different party of part or all of the rights and/or obligations contained or referenced in this Participation Agreement, the Business Rules or the Operating Rules.

### *2.7.13 Business Rules and Operating Rules Freeze*

The parties agree that the Business Rules or the Operating Rules are not intended to be, and shall not be amended for a period of one year from the date of execution of this Participation Agreement or before October 31, 2006, whichever date shall precede the other. However, by signed amendment to this Participation Agreement, the parties may modify this term as circumstances require.

## 2.8 Signatures

The undersigned represent and warrant that they have the requisite power and authority to execute this Participation Agreement on behalf of their respective organizations (the Parties), including authority to legally bind their respective organizations to the Binding Documents referenced in Section 3.3.3.2 of the Business Rules.

| _____ | _____ |
|---|---|
| Relying Party | GSA |

# 3 E-AUTHENTICATION FEDERATION INTERIM BUSINESS RULES

## 3.1 Title

This document shall be known and may be cited as the "E-Authentication Federation Interim Business Rules", or, as referenced herein, as "Business Rules".

## 3.2 Scope

### *3.2.1 Scope of Rules*

Signatories agree that their signed Participation Agreement, these Business Rules, the Operating Rules and the Binding Documents referenced in Section 3.3.3.2 herein, govern participation in the E-Authentication Federation, administered by the General Services Administration of the United States Federal Government (GSA). The GSA, or its authorized agent, shall approve Credential Services (CSs) of a Credential Service Provider (CSP). Approved Credentials of a GSA Approved CSP must be accepted, validated and relied upon by GSA Approved Relying Parties (RPs). Such acceptance, validation or reliance does not require the use of any additional contract between an Approved CSP and an Approved RP.

### *3.2.2 Agreements and Conduct Outside Scope of Rules*

Nothing in these Business Rules or the Operating Rules shall be construed to prevent Approved CSPs and RPs from executing such additional agreements among themselves as they see fit, including agreements covering the use of services, transactions or Credentials, including identity assertions or parts of such assertions. Any activity covered by other contract arrangements, other than the Participation Agreement, these Business Rules, the Operating Rules or other Binding Documents referenced in Section 3.3.3.2 herein, is subject to the terms of such other contract arrangements, and is outside the scope of these Business Rules. These Business Rules and the Operating Rules are incorporated by reference into the signed Participation Agreements and thereby applicable to the Signatories.

### *3.2.3 Rules Appearing in Multiple Documents*

Any provision of these Business Rules or the Operating Rules that duplicates or emphasizes identical or similar provisions of other Binding Documents referenced in Section 3.3.3.2 governing the E-Authentication Federation shall not be construed as to lessen the enforceability of any other provisions that have not been duplicated or emphasized.

## 3.3 Participation

### *3.3.1 Eligibility*

A department, Agency, Government sponsored corporation, or other instrumentality, or any State or Local Government is eligible to become a RP within the E-Authentication Federation, provided the requirements set forth in these Business Rules and the Operating Rules are satisfied.

A department, Agency, Government sponsored corporation, or other instrumentality, including a Designated Financial Agent of the United States Federal Government, or any State or Local Government is eligible to become a CSP within the E-Authentication Federation, provided the requirements set forth in these Business Rules and the Operating Rules are satisfied.

A CSP that is part of the Unites States Federal Government has the right to choose not to provide Credential Services to a RP that is not part of the United States Federal, State, or Local Government.

In addition, any legal entity, including a non-governmental organization, is eligible to become a CSP within the E-Authentication Federation provided the requirements set forth in these Business Rules and the Operating Rules are satisfied.

Any Signatory must continue to abide by the terms of their signed Participation Agreement to remain eligible to participate in the E-Authentication Federation.

### *3.3.2 Participation Requirements*

#### 3.3.2.1 Relying Parties

Approval by the GSA is necessary for a RP to participate in the E-Authentication Federation. A RP must be a Signatory as a prerequisite to approval by the GSA. A party becomes a Signatory RP by executing the Relying Party Participation Agreement with GSA. Each such Relying Party Participation Agreement includes obligations whereby these Business Rules and the Operating Rules, as periodically Approved in writing and amended in accordance with the change control process, are incorporated by reference. Final approval by the GSA is contingent upon the Signatory successfully completing the Boarding Process and Operational Readiness Review.

A Signatory RP must also be Approved according to terms of the Binding Documents referenced in 3.3.3.2, and comply with National Institute of Standards and Technology (NIST) SP 800-53 and the security requirements specified in the Operating Rules.

#### 3.3.2.2 CSPs

Approval by the GSA is necessary for a CSP to participate in the E-Authentication Federation. A party becomes a Signatory CSP by executing the CSP Participation Agreement with GSA. A CSP Participation Agreement may be executed directly with the GSA, or as part of a formal solicitation and procurement process the GSA may

require. Each such CSP Participation Agreement includes obligations whereby these Business Rules and the Operating Rules, as periodically Approved in writing and amended, are incorporated by reference.

A Signatory CSP must also have one or more CSs Approved according to the terms of the Binding Documents referenced in Section 3.3.3.2, herein, including the Credential Assessment Framework Suite (CAF), and be added to the E-Authentication Federation Trusted Credential Service Provider List as a prerequisite to be Approved by GSA to participate in the E-Authentication Federation.

#### 3.3.2.3 End-Users

Any party participating in the E-Authentication Federation as an End-User must have an agreement with an Approved CSP or an entity acting under an agreement, or chain of agreements, with an Approved CSP. Such agreement must contain such minimum terms as are required under these Business Rules and the CSP Participation Agreement. An End-User may be a natural person or any other legal entity, including a corporation. End-Users are Participants in the E-Authentication Federation, but are not Signatories.

### *3.3.3 GSA Role and Obligations*

The GSA is the party responsible for policy and operations related to the E-Authentication Federation. The GSA is responsible for facilitating the roles, relationships and mutual obligations among parties operating in the E-Authentication Federation. The GSA uses Business Rules, Operating Rules and Participation Agreements as a method of documenting these roles, relationships and obligations in a formal and, as needed, enforceable manner. The GSA shall provide processes for determining qualification of any party in the E-Authentication Federation. In the course of such activities, as well as ongoing oversight of Approved Parties and System performance, the GSA shall act as coordinator and policy enforcement body for the E-Authentication Federation. Any GSA approvals or other determinations required by or arising under these Business Rules and the Operating Rules shall not be unreasonably withheld. The GSA may designate offices, departments or other organizational units within the GSA or otherwise within the United States Federal Government to exercise such rights or obligations defined under these Business Rules and the Operating Rules.

#### 3.3.3.1 Operating Authorization

GSA actions in administering the E-Authentication Federation support the authentication component of the United States Federal Enterprise Architecture. The President's Management Agenda of 2001 directed GSA to lead the operation of the E-Authentication Federation, which implements Office of Management and Budget (OMB) M04-04 and NIST SP 800-63.

#### 3.3.3.2 Promulgation and Amendment of Business Rules, Operating Rules and Other Documents

GSA shall formalize the initial set of these Business Rules and the Operating Rules pursuant to its duty to administer and manage the E-Authentication Federation. Amendments to these Business Rules and the Operating Rules must comply with the E-Authentication Federation Change Management Policy. In addition to these Business Rules, the following materials are also formal Binding Documents defining rights, obligations, processes and other binding statements relative to the E-Authentication Federation: the CSP Participation Agreement, the Operating Rules, the Relying Party Participation Agreement, the Credential Assessment Framework (CAF), the Technical Architecture, and the Interface Specification.

#### 3.3.3.3 Relying Party and CSP Approval

The GSA is responsible for determining whether to approve a RP for participation in the E-Authentication Federation, and shall formalize and may amend periodically the requirements for RP approval. The GSA is responsible for determining whether to approve a CSP for participation in the E-Authentication Federation, and shall formalize and may amend periodically the requirements for CSP approval.

#### 3.3.3.4 Service Offerings

To promote use of the E-Authentication Federation, the GSA will facilitate policies for business relationship management, Business Rules, Operating Rules, Participation Agreements and other offerings, and will provide access to or make available various Architectural Components.

##### 3.3.3.4.1 Architectural Components

GSA may implement and make available to Approved Parties Architectural Components to facilitate use of the E-Authentication Federation, including the E-Authentication Portal identified in the Technical Architecture, Step-Down Translator(s), Schema Translator(s) and Validation Services. The GSA may incorporate additional components.

##### 3.3.3.4.2 Interoperability Requirements

The GSA shall operate an interoperability laboratory for the purpose of testing interoperability of products, software, communication specifications and other relevant aspects of current and potential future enhancements to the E-Authentication Federation. Each Signatory CSP and RP shall be responsible for the completion of their own testing in such laboratory in accordance with Section 3.3.6.2 of these Business Rules.

##### 3.3.3.4.3 Federation Operations Center

The GSA shall operate a Federation Operations Center.

##### 3.3.3.4.4 Trusted Credential Service Provider List

The GSA shall formalize, maintain and update as needed a Trusted Credential Service Provider List of Approved CSPs participating in the E-Authentication Federation. This

list shall be a public document and include, at a minimum, the names of each CSP that has been successfully Approved, and the Assurance Level of each Approved CS of that CSP. The GSA shall determine what continuing audit and other compliance requirements shall satisfy maintenance of approval and the terms of these Business Rules and the Operating Rules.

#### 3.3.3.5 Contact Information

For current information related to the E-Authentication Federation and these Business Rules, contact the E-Authentication Program Director of the General Services Administration of the United States Federal Government or see http://www.cio.gov/eauthentication/.

### *3.3.4 Relying Party Role and Obligations*

#### 3.3.4.1 Relying Party Boarding Process, Operational Readiness Review and Participation Agreement

As a prerequisite to be Approved to participate in the E-Authentication Federation, a RP is obliged to successfully complete the Boarding Process and Operational Readiness Review, and to execute a Relying Party Participation Agreement with the GSA, thereby agreeing to abide by these Business Rules, the Operating Rules and other Binding Documents referenced in Section 3.3.3.2 of the Business Rules. The Relying Party Participation Agreement incorporates these Business Rules and the Operating Rules by reference.

#### 3.3.4.2 Interface Specifications, Approved Software Use and Upgrade

A RP is obliged to comply with and use the E-Authentication Interface Specification to participate in, communicate through or connect with the E-Authentication Federation. A RP is obliged to use software on The Approved Technology Provider List or interface software otherwise Approved by GSA. In order to maintain approval to participate in the Federation, each RP is obliged to follow requirements set by GSA to stay current with the software on The Approved Technology Provider List.

#### 3.3.4.3 Security and Privacy Compliance

The following Rules apply to any information System supporting the Agency Application (AA) of the RP that is part of the United States Federal Government. An Approved RP is obliged to comply with OMB Circular No. A-130 including Appendix III to OMB Circular No. A-130, with respect to any information technology System of the RP.

An Approved RP is obliged to comply with the Privacy Act of 1974 and OMB M-03-22, including where required, performing a Privacy Impact Assessment (PIA) with respect to the handling of Personally Identifiable Information (PII) of an End-User.

An Approved RP that is not part of the United States Federal Government must prove to the GSA that it is in compliance with equivalent safeguards and relevant requirements. GSA, in its discretion, shall determine whether such approval is sufficient.

#### 3.3.4.4 Reasonable Reliance on Credential

A RP is obliged to reasonably determine for itself whether to rely on the authentication status of an End-User and whether to authorize usage of the AA. In order to determine the authentication status of an End-User, a RP must determine for itself, either through a published Activation process or other procedures, the level of AA Risk, and therefore the needed Assurance Level, as per the guidance in OMB M-04-04 and NIST SP 800-63, using the GSA-provided Electronic Risk and Requirements Assessment (E-RA) tool or any other method it deems acceptable.

### *3.3.5 CSP Role and Obligations*

#### 3.3.5.1 CSP Boarding Process, Operational Readiness Review and Participation Agreement

To be an Approved CSP, a CSP must successfully complete the Boarding Process and Operational Readiness Review, including being added to the Trusted Credential Service Provider List. A CSP is also obliged to execute a CSP Participation Agreement with the GSA as a prerequisite to being an Approved CSP for participation in the E-Authentication Federation, thereby agreeing to abide by these Business Rules, the Operating Rules and other Binding Documents referenced in Section 3.3.3.2 of these Business Rules. The CSP Participation Agreement incorporates these Business Rules and the Operating Rules by reference.

#### 3.3.5.2 CSP Continuing Audit Requirement

An Approved CSP is obliged to undergo an audit, no less than annually, confirming compliance with continuing requirements arising out of approval and with the obligations and other relevant terms of these Business Rules, the Operating Rules and the CAF. An audit planned or undergone by a CSP unrelated to the E-Authentication Federation, including an internal audit, may be sufficient to meet this requirement in whole or in part, in the discretion of the GSA. The scope of an audit shall be limited to a CSPs conformance with the Business Rules, Operating Rules, and other Binding Documents. An Approved CSP must report to GSA in a timely manner any negative finding by an auditor that is material to compliance with requirements under any Binding Document referenced in Section 3.3.3.2.

#### 3.3.5.3 Material Change to CSP, Credential Services or Credential

An Approved CSP may be required by the GSA to undergo an additional approval in whole or in part, to re-approve one or more CSs at the same or different Levels of Assurance or to accept suspension or termination of approval and participation in the E-Authentication Federation when audit results indicate material changes in the CSP, the

Approved CSs or in the Credentials it issues or other relevant changes that bring the CSP out of material compliance with continuing requirements.

#### 3.3.5.4 Technical Architecture and Interface Specification

To participate in, communicate through or connect with the E-Authentication Federation, a CSP is obliged to comply with, implement and use the E-Authentication Technical Architecture, the E-Authentication Interface Specification, and all other applicable technical requirements identified in any Binding Document referenced in Section 3.3.3.2 of the Business Rules.

#### 3.3.5.5 Designated Financial Agents

Notwithstanding any prohibition on assignment of rights contained in any Binding Document referenced in Section 3.3.3.2 of these Business Rules, the Department of the Treasury, in its role as a CSP, may designate one or more entities to act as its agent, provided that each such agent is fully subject to all Rules, rights, obligations contained within the CSP Participation Agreement, these Business Rules, the Operating Rules, any other Binding Document referenced in Section 3.3.3.2 of these Business Rules and any other relevant document, practice or procedure of the E-Authentication Federation applicable to an Approved CSP.

CSPs whether principals or agents for CSPs shall be held individually accountable for compliance with Business and Operating Rules.

### *3.3.6 General Obligations*

Every Approved Party is obliged to comply with the following Rules.

#### 3.3.6.1 Federation Security and Reliability

Every Approved Party agrees to coordinate with the GSA in safeguarding the security and reliability of the E-Authentication Federation. GSA may render inaccessible any Node or Architectural Component of the E-Authentication Federation to prevent or cease serious harm to the Federation. Every Approved Party may disable their connection to any Node or Architectural Component of the E-Authentication Federation to prevent or cease serious harm to their Systems or to the Federation. Every Signatory agrees to provide notice to the counter-party Signatory of their Participation Agreement of any such emergency suspension of service prior to, if practicable, or as soon after as reasonably possible. Participation by any Approved Party in the E-Authentication Federation may be suspended under extraordinary circumstances necessary to prevent or cease serious harm to the E-Authentication Federation.

#### 3.3.6.2 Federation Interoperability

To assure the efficacy and operation of the E-Authentication Federation, every Approved Party must demonstrate to the GSA that its interactions and communications through the Federation comply with the E-Authentication Technical Architecture and will

interoperate with the Architectural Components of the Federation. To this end, every Approved Party must conduct tests of its planned Federation interactions and communications in the Interoperability Lab, or through such other process GSA may designate, to demonstrate compliance and interoperability requirements for the Federation have been met.

#### 3.3.6.3 Operational and Ongoing Requirements

Every Approved Party is obliged to comply with application, testing, piloting, production and continuing maintenance requirements set forth by the GSA. These ongoing requirements include continued compliance with the provisions of the CAF, NIST SP 800-53, the security requirements specified in the Operating Rules, and with applicable requirements documents defining operational sufficiency for participation in the E-Authentication Federation. Nothing in this section, however, shall be construed to prevent any Approved Party from extending, adding to or otherwise applying other technologies or services in accordance with Section 3.2.2 of these Business Rules.

#### 3.3.6.4 End-User Consent and Notice

Every Approved Party is obliged to assure that each End-User that is an individual natural person has provided Informed Consent to the sharing of any PII related to such End-User by the Approved Party with any other party operating within the E-Authentication Federation, including any PII contained in a certificate or other identity assertion as included in the Interface Specification. Under these Business Rules, no Approved CSP or Approved RP is permitted to share PII about any such End-User beyond the information provided for in the Interface Specification. Nothing in this section authorizes the sharing of PII about such End-User for purposes of sending commercial solicitations to that user, including marketing or advertising messages.

Every Approved CSP must inform each of its End-Users, prior to the End-User's participation in the E-Authentication Federation, that the End-User must maintain the security of their Approved Credential, including any Token housing their Credential, and must report to the CSP any known or reasonably suspected compromise of such Credential or Token.

In accordance with the Right to Financial Privacy Act, any financial institution providing CSP services must inform each End-User of the categories of information that will be disclosed (name, date of birth, etc.) and obtain the consent of the End-User to disclose that information to the Government. This requirement applies regardless of whether the financial institution is acting on its own or on behalf of a Government Agency.

Every Approved CSP must obtain the affirmative manifestation of assent by each End-User to the foregoing terms, prior to End-User participation in the E-Authentication Federation.

In the case of organizational End-Users, all relevant rights and obligations, including notice requirements and requirements for Informed Consent, must pass through to each natural person acting on behalf of End-User within the E-Authentication Federation.

To the extent that information identified as part of the Dispute Resolution processes described in the Participation Agreements constitutes PII within a System of Records under the Privacy Act of 1974, nothing in those agreements shall be construed to authorize or permit the communication of such information about an End-User who is an individual natural person without that End-User's Informed Consent.

#### 3.3.6.5 Additional Transactions

Approved Parties may conduct transactions and communicate data in conjunction with the E-Authentication Federation in addition to the authentication of an End-User. These additional transactions may be conducted in conjunction with the E-Authentication Federation, but will not be deemed to be within the scope but shall conform with the spirit of the Business Rules and the Operating Rules.

Acceptance of data by an Approved Party shall constitute an agreement for purposes of this subsection.

Notwithstanding the above, the following subsection applies to any such additional transaction.

##### 3.3.6.5.1 Transaction Privacy

Any additional transaction data transferred from an Approved CSP to an Approved RP shall be used solely for the purpose of the agreed transaction and related application and for resolving issues which may arise in the execution of that service. Such data shall not be used or forwarded to any other Government Agency or other party without the written approval of the Approved CSP. Such data shall also be kept only as long as required to perform the defined service, or unless required by applicable laws or other regulations. The Approved RP shall only store and maintain such data in their record keeping Systems once the End-User has verified the information and affirmatively manifested assent, in accordance with any applicable processes and policies of the Approved RP.

# 4 E-AUTHENTICATION FEDERATION INTERIM OPERATING RULES

## 4.1 Introduction

Public trust in the security of information exchanged over the Internet plays a vital role in the E-Gov transformation. The General Services Administration (GSA) makes that trust possible. As part of the President's Management Agenda, the E-Authentication Federation will ultimately enable trust and confidence in E-Government transactions through the establishment of an integrated policy and technical infrastructure for electronic authentication. Through the Federation, citizens and businesses will have simpler access to multiple Agency Applications (AAs) through the re-use of Credentials and established identities. Furthermore, GSA will establish a Federation comprised of Relying Parties (RPs) and Credential Services (CSs).

The E-Authentication concept is best described through the trust relationships among AAs, Credential Service Providers (CSPs) and End-Users. CSPs are commercial or Government entities authorized by GSA to provide Credentials (e.g., Personal Identification Numbers (PINs), Passwords, Digital Certificates) to potential End-Users for access to Government Systems. AAs are Government applications, Systems or services that rely on (or trust) the authentication/ CS of CSPs. End-Users are people or organizations that have Credentials issued by a CSP and desire to use that Credential to conduct business with an AA. It is the management of trust among these entities (AA, CSPs and End-Users), that is the essence of the Federation.

### *4.1.1 Purpose*

This document defines operational requirements for Federation Members. The Operating Rules defined herein ensure that the best interests of the Federation, specifically the Integrity of the operating environment, are maintained. Operating Rules are in addition to requirements specified in various documents that are identified within the body of this document. Where necessary, these documents are referenced and several of the documents are included as an appendix to this document.

The Operating Rules described herein are ***mandatory*** except for those that explicitly grant latitude or subjective judgment or where official waiver is granted by GSA. Federation Members are required to formally agree to these Operating Rules. End-User requirements are to be provided by Federation Members and are not within the scope of this document.

### *4.1.2 Document Organization*

This document provides specific areas that a Federation Member must implement. The document is organized according specific Operating Rules and is subsequently broken down into specific requirements for each area. Where necessary, additional requirements are identified by reference and the appropriate document is listed. This document also

contains several appendices that provide supporting information or references that are defined within the body of the Rules.

## 4.2 Privacy

End-User privacy is a high priority for GSA. Federation Members must strive to protect End-User privacy at all times. The following Rules apply:

| Reference Number | Privacy |
|---|---|
| 4.2.1 | PII may be provided to RPs for establishing End-User identity; no other use of this information is permitted unless:<br>1. The CS provides written consent to the RP, and<br>2. The End-User provides explicit permission to the CS. |
| 4.2.2 | Federation Members must comply with all privacy laws and regulations as applicable, whether or not referenced specifically by Federation Rules and guidance. |
| 4.2.3 | Federation Members must comply with the Privacy Act of 1974 to the extent applicable. |

## 4.3 Logs

Federation Member Systems and applications will need to produce particular log records. To maintain a level of security and consistency across the Federation, the following Rules apply:

| Reference Number | Logs |
|---|---|
| 4.3.1 | Assertion-based RPs must log transaction identifier (TID)[1], CS identifier (CSID), End-User identifier (UID), assertionid, Assurance Level, and subject name (commonName) for every assertion received. |
| 4.3.2 | Assertion-based RPs should log artifacts and every element in the assertion[2]. |
| 4.3.3 | CSs sending Security Assertion Markup Language (SAML) assertions must log assertionid, UID, and TID for every assertion. |
| 4.3.4 | Assertion-based Federation Members must have the ability to correlate local session identifiers with associated authenticated transactions. |
| 4.3.5 | CSs sending SAML Assertions should log artifacts and all assertion elements. |
| 4.3.6 | Certificate-based RPs must log the End-User certificate and relevant validation activities. |
| 4.3.7 | RPs must be able to track the activity of End-Users from the receipt of external authentication through the end of the Business Transaction[3]. |
| 4.3.8 | Federation Members must have processes and controls that ensure that System Log Files can be used as persuasive evidence in a court of law[4]. |
| 4.3.9 | The Federation Portal will record TID, CS selected, and AA selected at the Portal. |
| 4.3.10 | All logs relevant to these Rules must include a date and timestamp for every log entry. |
| 4.3.11 | CSPs must keep the logs defined in these Rules in accordance with Federal, State, Local and regulatory requirements or a minimum of 3 years. |
| 4.3.12 | RPs must keep related logs of transactions in accordance with Federal, State, Local and regulatory requirements or a minimum of 3 years. |
| 4.3.13 | Production environment logs required by these Rules must be backed up, including the use of on offsite storage location that has appropriate environmental and security controls. |

## 4.4 Reporting

Communication amongst Federation Members is a key component of the operations of the Federation. GSA may share information required in this section with Connected Members. The following reporting Rules apply:

| Reference Number | Reporting |
|---|---|
| 4.4.1 | RPs must provide a monthly report containing each authenticated session, which should be ASCII-encoded text in comma-separated values format. Contents are as follows:<br>1. Timestamp - Must include date and time. Time should be specified in Greenwich Mean Time (GMT) and include hours, minutes, and seconds. Will have the format mmddyyyy:hh:mm:ss .<br>2. TID - Will have the format P-mmddyyyy-{luid}. The luid is a base64 encoded representation of 64 bits that is unique to a transaction.<br>3. AAID - As published in the Federation Metadata.<br>4. CSID - As published in the Federation Metadata; if a certificate is used, the contents of this element should consist of the issuer of the certificate presented by the user.<br>5. Assertion Validation (success/failure) - Should represent the successful receipt of an assertion or successful validation of the presented end-user's certificate. Values: 0 = Failure & 1 = Success. |
| 4.4.2 | CSPs must provide a monthly report containing each authenticated session, which should be ASCII-encoded text in comma-separated values format. Contents are as follows:<br>1. Timestamp - Must include date and time. Time should be specified in GMT and include hours, minutes, and seconds. Will have the format mmddyyyy:hh:mm:ss.<br>2. TID - Will have the format P-mmddyyyy-{luid}. The luid is a base64 encoded representation of 64 bits that is unique to a transaction.<br>3. AAID - As published in the Federation Metadata.<br>4. CSID - As published in the Federation Metadata.<br>5. Assertion Validation (success/failure) - Should represent the successful, completed transmission of an assertion. Assertions that are not fully transmitted must be considered to have failed. Values: 0 = Failure & 1 = Success. |
| 4.4.3 | GSA will publish reports on the Federation Portal traffic to the Federation every month via means accessible only to active Federation Members in good standing. Reports will include the number of page views and the number of transactions initiated. |

| | |
|---|---|
| 4.4.4 | GSA will provide Federation activity reports to Federation Members every month via means accessible only to active Federation Members in good standing. Reports will include the total number of Federation authenticated sessions. |
| 4.4.5 | All reports will be a signed and encrypted Secure/Multipurpose Internet Mail Extension (S/MIME) email using digital certificates that are trusted by the Federation[5] until the email is incapable of handling the data (i.e. size). |

## 4.5 Monitoring

To ensure that the System maintains a level of security, Integrity and Availability, a certain level of monitoring must occur. The following Rules provide a minimum set of requirements for achieving the level of monitoring necessary to maintain the Federation. The following Rules apply:

| Reference Number | Monitoring |
|---|---|
| 4.5.1 | GSA will publish monitoring service information, such as IP address, location, and contact information, at least two (2) weeks in advance of the start of monitoring or the implementation of changes in monitoring service. |
| 4.5.2 | GSA, or its designated representative, will monitor the Availability of the Federation Member's web-based E-Authentication-enabled applications during the agreed upon hours of operation, to ensure that the services are being delivered to end-users according to the standards contained in Section 4.9 and Appendix D. |
| 4.5.3 | Federation Members must monitor the Availability of their own web-based E-Authentication-enabled applications in accordance with Section 4.9 and Appendix D. |
| 4.5.4 | GSA reserves the right to use third parties to run tests and to change monitoring tools at its sole discretion, provided the scope of such tests be mutually agreed between Federation Members and GSA and subject to the terms of this agreement. |
| 4.5.5 | All tests must be targeted at "top level" load balancing Uniform Resource Locators (URLs) and URLs will be selected based on the criticality of functionality to the Federation Portal and will be designed to exercise components of Federation's infrastructure involved in delivery of the services provided by Federation RPs[6]. |
| 4.5.6 | Compliance with the terms of Section 4.9 and Appendix D will be evaluated based on the Availability of the services provided by Federation RPs and CSs. |
| 4.5.7 | Data collected from all tests will be evaluated using three different methods: Availability, minimum acceptable response time, and average response time (see Appendix D). |
| 4.5.8 | GSA's measurements of performance and Availability compliance data will be available to Connected Members[7]. |
| 4.5.9 | On a monthly basis, all testing evaluation methods must pass to be considered in compliance, based on the criteria in Appendix D and the measurements made by GSA. |

| | |
|---|---|
| 4.5.10 | If measurements made by GSA leads to a determination of non-compliance (fail), a joint analysis will be conducted to determine the source of the situation. The Federation Member and GSA will work to resolve the situation if it is in either's control. Otherwise the Federation Member will be deemed compliant. This joint determination will be made prior to disseminating or publishing compliance and Availability information to Connected Members. |
| 4.5.11 | Federation Members do not need to pass every periodic test for every window in order to pass on a monthly basis (see Appendix D). |
| 4.5.12 | A failure to pass any of the three testing evaluation methods on a monthly basis will constitute non-compliance for the month. |
| 4.5.13 | Tests will be run at five-minute intervals and tests may be run from monitors located within GSA hosting sites or from external monitors. |
| 4.5.14 | For external monitors, tests will be run from at least three domestic locations. |
| 4.5.15 | Certain time frames, testing locations or URLs may be exempt from calculation for a variety of reasons: testing location unavailable, tech window, change window, mutually agreed scheduled maintenance windows, etc., or Internet problems beyond the reasonable control of either party. |
| 4.5.16 | Exempt items will be excluded from the Availability and performance compliance calculations. |

## 4.6 Performance Requirements

Availability of the Federation is critical and this section provides Federation Member performance requirements. Appendix D also provides test and measurement criteria that Federation Members should use as a guide when implementing performance requirements. Performance degradation will be treated as an incident described in Section 4.9. The following Rules apply:

| Reference Number | Performance |
|---|---|
| 4.6.1 | All Federation Member services must achieve 99% Availability during scheduled up time as defined by the Federation Member. |
| 4.6.2 | Federation Members must ensure routine maintenance requiring downtime must not be scheduled 6 a.m. to 9 p.m. (Eastern Time (ET)) Monday through Friday. |
| 4.6.3 | Federation Members must provide planned up time and downtime schedules to GSA, and GSA will provide them to the Connected Members. |
| 4.6.4 | Federation Members must monitor their own sites for Availability and response time. |
| 4.6.5 | Federation Members must notify GSA of any unscheduled downtime as soon as detected in compliance with escalation policies defined in Section 4.9. |
| 4.6.6 | Response time will include Domain Name System (DNS) resolution, connect (i.e., TCP 3-way handshake), and 1st byte transferred. |
| 4.6.7 | Federation Members will be monitored by GSA to ensure Availability and adequate response times[8]. |
| 4.6.8 | GSA will conduct tests using the test criteria listed in Appendix D. |
| 4.6.9 | GSA shall ensure the Federation Portal is available 99.9% of the time, 24x7. |
| 4.6.10 | GSA shall ensure that E-Governance Certificate Authority (E-GCA) revocation data is available 99.9% of the time, 24x7. |
| 4.6.11 | Federation Members will display down pages during planned or unplanned service unavailability. |

## 4.7 Style Guidelines, Narrative Elements, Branding and Logos

GSA will establish, provide, and maintain Federation Style Guidelines, which will include Approved content for use on Federation Member sites. Use of Federation Member branding and logos is subject to the intellectual property terms defined in Section 1.7.8 (CSPs) and 2.7.3 (RPs). This section provides requirements for Web sites linking to the Federation Portal in terms of presenting visual and narrative elements that identify those sites as Members of the Federation. The following Rules apply:

| Reference Number | Style Guide and Narrative Elements |
|---|---|
| 4.7.1 | Federation Member sites must contain language that describes and explains E-Authentication in a manner consistent with the language loaded on to the Federation Portal page.<br>1. GSA will provide an "E-Authentication Primer," which Federation Members may display in whole or in part from their sites.<br>2. This Primer must be accessed via a clear link that leads to:<br>a. A page within the Federation Member's site; or<br>b. A pop-up window off the Federation Member's site; or<br>c. The Federation Portal in a separate window. |
| 4.7.2 | Federation Member sites must contain language that describes and explains E-Authentication in a manner consistent with the language loaded on to the Federation Portal page.<br>1. GSA will provide an "E-Authentication Frequently Asked Question (FAQ)," which Federation Members may display in whole or in part from their sites.<br>2. This FAQs must be accessed via a clear link that leads to:<br>a. A page within the Federation Member's site; or<br>b. A pop-up window off the Federation Member's site; or<br>c. The Federation Portal in a separate window. |

| Reference Number | Style Guide and Narrative Elements |
|---|---|
| 4.7.3 | Federation Member sites must provide explanatory / educational references to the Federation Portal and related processes at site pages that link directly to the Portal.<br>1. In the case of RPs, this means at a minimum the page from which the user is sent to the Federation Portal to select a CS.<br>2. In the case of the CSP, this means at a minimum the page from which a user is sent to the Federation Portal to select Government service, or RP, from which to access services.<br>3. GSA will provide Federation Members a copy of the pages that will be used as appropriate in whole or in part. |

| Reference Number | Branding and Logos |
|---|---|
| 4.7.4 | Federation Members must display the Federation logo. |
| 4.7.5 | Only those sites explicitly authorized by GSA may display the Federation logo.<br>1. All Federation Member Websites.<br>2. Non-Federation Member sites may also be authorized at the discretion of GSA.<br>3. GSA will provide electronic files containing the logo to authorized parties. |
| 4.7.6 | The logo must be displayed unmodified, unless modification is explicitly Approved by GSA. |
| 4.7.7 | The logo must be displayed on each page of the Federation Member's site that links directly to the Federation Portal. |
| 4.7.8 | The logo must be displayed on each page within the Federation Member site that lists partner or affiliate Web sites / services. The logo must not be conveyed by a Federation Member site to any partner or affiliate Web site / service, even if that site is also a Federation Member. |
| 4.7.9 | The logo will be made available in .jpg and .gif format. |
| 4.7.10 | Maximum size specification for use at the Federation Member site is:<br>• Width: 140 pixels<br>• Height: 40 pixels |

| Reference Number | Branding and Logos |
|---|---|
| 4.7.11 | Federation Member logos will be made available to GSA in .jpg and .gif format. |
| 4.7.12 | Maximum size specification of the Federation Member logo is:<br>• Width: 140 pixels.<br>• Height: 40 pixels. |
| 4.7.13 | Federation Members must provide GSA with branding information, including logos, solely for use in the Federation Portal. This material will be provided and used unaltered. |
| 4.7.14 | Federation Members must use Federation branding information only as allowed in these Federation Style Guidelines. |
| 4.7.15 | Federation Members must not use other Federation Members branding information without explicit written permission from the Federation Member. |

## 4.8 Security Requirements

The security requirements are intended to protect and secure Federation Member information assets and application Systems from threats, whether internal or external, deliberate or accidental. They aim to ensure the Availability, Integrity, and Confidentiality of information to the extent required by GSA. The objectives of the requirements are:

- To ensure that GSA information assets such as Federation Member and transaction information are pragmatically protected on a cost-effective basis and to a level that allows the Federation to fulfill its mission and operate within acceptable levels of Risk to information assets.
- To provide an indication of the mandatory provisions that should be adhered to.
- To establish standards for the means by which information exchanged with Federation Approved Parties will be controlled and safeguarded.

This section defines the minimum-security requirements throughout the Federation System and provides a template for consistent application of these requirements. The security requirements are organized by area. The following Rules apply:

| **Reference Number** | **General** |
|---|---|
| 4.8.1 | CSPs must comply with the requirements of the Credential Assessment Framework (CAF) Suite. |
| 4.8.2 | RPs must attest to compliance with National Institute of Standards and Technology (NIST) SP 800-53 as required by Federal Information Security Management Act (FISMA). |
| 4.8.3 | Security requirements for protocols and messaging are included in the E-Authentication Interface Specifications. Federation Members must comply with the requirements of the interface specifications. |
| 4.8.4 | Federation components operated by GSA must abide by the FISMA and GSA Information Technology (IT) Security Policy, CIO HB 2100.1A. |

| **Reference Number** | **Confidential Information and Electronic Messaging** |
|---|---|
| 4.8.5 | All confidential information shall be marked as confidential by the data/information owner, and the receiver shall protect it as such unless otherwise specified by these Operating Rules. |

| Reference Number | Confidential Information and Electronic Messaging |
|---|---|
| 4.8.6 | For the purposes of these Rules, confidential information will be defined as whatever is marked as confidential by the information owner. |
| 4.8.7 | All Federation Member personnel who have access to, or are authorized to work on Systems/devices processing or storing, End-User data and/or confidential information must participate in a suitable background evaluation that includes financial and criminal record checks. |
| 4.8.8 | Federation Members must employ security measures to safeguard confidential information that is being stored, processed, transported, or disposed. These measures must apply to paper files, tape backups, call logs, mail messages and other media. |

| Reference Number | Security Policies and Procedures |
|---|---|
| 4.8.9 | GSA, or its authorized representatives, will have the right to perform a review of Federation Member's relevant security, business continuity, data center and operations controls (at GSA's own expense) in response to a security incident.<br>1. Federation Members must grant GSA and its representatives reasonable access, subject to the Federation Member's standard security policies, during normal business hours and upon two (2) weeks notice, to the relevant portion of the Federation Member's records and facilities as they relate to their Participation Agreement.<br>2. Federation Members must provide GSA, or its authorized representatives, such information and assistance as reasonably requested in order to perform such a review. |

| Reference Number | Security Policies and Procedures |
|---|---|
| 4.8.10 | Federation Members must allow GSA, or its designee to perform regular reasonable Network, security vulnerability assessments on any of the Federation Member's Internet accessible Systems and servers utilized by the Federation Member that host Federation confidential information in order to measure vulnerability of the Network to external cyber attack. A list of externally facing Systems must be provided to GSA and updated as changes occur.<br>1. GSA and the Federation Member will work to establish mutual agreement on date and time of security scans.<br>2. Two (2) weeks prior to performing the assessment, GSA will provide the Federation Member with the following information:<br>• Date, time, and duration of security scan;<br>• IP address performing the test; and<br>• Name, phone number and pager of person performing the scan.<br>3. No destructive or intrusive testing (brute force or denial-of-service (DOS)) will be performed.<br>4. As the servers utilized by the Federation Member are Internet accessible, any user on the Internet can perform these tests, so long as the tests will not have a negative impact on the Federation Member's Network or data center.<br>5. GSA will have support available to address any negative consequences as a result of the assessment. |
| 4.8.11 | GSA will provide each Federation Member access to the security reports produced as part of the review of that Federation Member's security controls and the security vulnerability assessments, and the Federation Member agrees to take commercially reasonable steps to address the concerns contained in such reports within timeframes mutually agreed to by the Federation Member and GSA. Federation Members must track the actions taken to address any concerns contained in the security reports to ensure the agreed upon changes are implemented as agreed to and must report the progress of such actions to GSA. |
| 4.8.12 | Federation Members must mitigate against known vulnerabilities on Systems providing services to the Federation. Acceptable mitigation may consist of active remediation (e.g., patches, coded updates, firewall changes, etc.). |
| 4.8.13 | GSA must be notified of any proposed modifications that may materially impact a Federation Member's overall security posture at least ten (10) business days prior to implementation. |

| Reference Number | Security Policies and Procedures |
|---|---|
| 4.8.14 | Federation components operated by GSA must comply with GSA security policies and procedures, including Certification and Accreditation (C&A). |

| Reference Number | System Security |
|---|---|
| 4.8.15 | Federation Members, their contractors, and their agents must ensure that all sensitive and confidential information is secured against unauthorized access. |
| 4.8.16 | When outside a firewall and attempting to access a Federation System root, strong authentication procedures (i.e., two-factor authentication, such as use of Password & hard Token or a passcode & biometric System) are required. |
| 4.8.17 | Federation Members will ensure that Systems Passwords are sufficiently complex (e.g., length, construction, frequency of change, etc.) to reduce the likelihood of System Password compromise. |
| 4.8.18 | All System access will be configured by the Federation Member to prevent an intruder from gaining access to the System. |
| 4.8.19 | All transaction requests denied access must not reveal detailed information about the Federation Member's hardware/software configuration. |
| 4.8.20 | All user input and data, including URL name-value arguments, will be checked for its appropriateness based on its format, size and validity and any inputs not conforming to those parameters must be rejected. |
| 4.8.21 | The servers utilized by Federation Members will not have the ability to remotely execute arbitrary outside requests, except for remote management performed over an encrypted, authenticated channel. |
| 4.8.22 | For Internet exposed Systems providing services to the Federation, the following Rules apply:<br>1. All routers used within Federation Member Systems are to be segmented to provide a Federation Member's Network traffic in isolation of other Network traffic; the Federation Member's segment contains a packet filter which has been configured to disallow access to all protocols.<br>2. When a protocol (such as http and https) is allowed to call into the Federation Member System, that protocol must be explicitly exceptioned into the firewall infrastructure. |
| 4.8.23 | Monitoring procedures of the firewall and supporting Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) will promptly inform Federation Members of any unauthorized access or otherwise suspicious attempts to access secured portions of the System across the Network. |

| Reference Number | System Security |
|---|---|
| 4.8.24 | Federation Member's Systems must have logging enabled and sufficient information must be captured in the logs to provide for individual accountability of all access to, or attempts to access, the data stores that contain confidential information. |
| 4.8.25 | Systems storing or processing sensitive and confidential information must be stripped and be configured with only enabled services and must have unnecessary and unused services disabled. It is recommended that unneeded services be removed. |

| Reference Number | Physical Access Control |
|---|---|
| 4.8.26 | Federation Members must implement physical Access Controls to secure access to the location, computer room(s), computer equipment and confidential information, including those locations managed by third party data centers. |
| 4.8.27 | Sensitive areas, such as data centers, must be monitored 24x7. |
| 4.8.28 | Systems storing or processing confidential information must be physically isolated and access must be granted to only authorized personnel. |
| 4.8.29 | Access must be removed from terminated and transferred employees prior to or upon termination or transfer. |
| 4.8.30 | All access to such areas storing or processing confidential information must be logged for audit purposes and made available to GSA during the conduction of security inspections. |
| 4.8.31 | Unauthorized access or access attempts, or other significant security incidents, resulting in breaches of the Federation Member's physical Access Controls must be reported to GSA after a Federation Member obtains knowledge of such events in accordance with the time frame set forth for severity one incidents (See Section 4.9). |
| 4.8.32 | Federation Members must use commercially reasonable efforts to terminate any breaches of its physical Access Controls immediately after detection. |

## 4.9 Incident Response

This section defines the requirements for managing an incident. An incident is an event that has a material adverse affect on a Federation Member System or service including but not limited to the following:

- Unwanted disruption or denial of service;
- Unacceptable site performance or Availability;
- The unauthorized use of a System for the processing or storage of data; or
- Unauthorized changes to System hardware, firmware, or software characteristics.

Incidents can take many forms and the following Rules apply:

| Reference Number | Incident Response |
|---|---|
| 4.9.1 | All Federation Members are responsible for reporting any known security incident promptly to GSA according to the escalation procedures that will be published periodically. |
| 4.9.2 | For any significant security incident that has led to a breach or compromise of sensitive and confidential information. Federation Members must present GSA with documentation of the cause of the security incident, remedial steps, and future plans to prevent a recurrence of the security incident. |
| 4.9.3 | When GSA initially detects a problem or a CSP or RP reports a problem or incident, GSA in consultation with the Federation Member, will first classify the problem or incident according to its severity and nature in accordance with the severity table located in this section. |
| 4.9.4 | When GSA becomes aware of an error or problem, either on its own accord or following notification made by a Federation Member, GSA will respond using the criteria listed in this section. |
| 4.9.5 | GSA will use commercially reasonable efforts to contact the Federation Member's technical contacts via telephone, pager, and email whenever an incident occurs. |
| 4.9.6 | GSA will provide the escalation contacts in regards to outages or change management in accordance with the Federation Change Management Policy. |
| 4.9.7 | Contact information must be provided to GSA, who may provide it to Connected Members. |
| 4.9.8 | For any incident, including dispute resolution, occurring in the last six (6) weeks, Federation Members must be capable of accessing relevant logs for forensic analyses within 24 hours. |

| Reference Number | Incident Response |
|---|---|
| 4.9.9 | For any incident that is six (6) weeks or older, Federation Members must be capable of accessing relevant logs for forensic analyses within 72 hours. |
| 4.9.10 | Escalation procedures for responding to security incidents that affect, or could reasonably be expected to affect, Federation's confidential information or any Systems on which the information is stored or processed, are set forth in these Operating Rules.<br>1. Without limiting the forgoing, Federation Members must notify GSA of any significant security incident (significant security incidents must be deemed to include, without limitation, any known attacks on or improper disclosure of Personally Identifiable Information (PII), Personal Health Information or any other personally identifiable End-User data) that breaches, compromises or threatens the Confidentiality, Integrity and/or Availability of GSA confidential information within the time frame set forth for Severity One incidents.<br>2. Federation Members must use reasonable business efforts to respond to security incidents and keep GSA informed of the incident, actions taken to respond to it and measures taken to correct it in accordance with the incident management procedures set forth in this section.<br>3. At no time must the Federation Member allow any security breach or compromise to persist for any amount of time in order to determine the identity of the perpetrator or for any reason, except as required by law or as deemed necessary to stop the compromise. |
| 4.9.11 | For any significant security incident that has led to a breach or compromise of the Federation's sensitive information, Federation Members must present GSA with documentation of the cause of the security incident, remedial steps, and future plans to prevent a recurrence of the security incident in accordance with the incident management procedures set forth in these Operating Rules.<br>If a Federation Member's proposed measures are not deemed acceptable, based on GSA's reasonable judgment, Federation Members must, upon receipt of written request from GSA, enter into good faith negotiations to address the differences and provide security fix within the time frames for providing solutions set forth in these Operating Rules. |

The following classification scheme will be used to categorize problems:

| Classification | Criteria |
|---|---|
| **Severity One:** | **Business Critical Failures**<br>• Issues that result in the outage of the entire service provided by GSA under this Agreement to the End-Users.<br>• Any situation that prevents new End-Users from accessing or using the applicable Customized Pages or the Tools, or existing End-Users from receiving their End-User data.<br>• Issues or software defects that result in a significant security exposure (i.e., disclosure to unauthorized third parties of personally identifiable health information of End-Users or other personally identifiable End-User data).<br>• Significant End-User data quality issue (missing, incomplete or incorrect End-User data with significant impact on End-User experience or on the Integrity of End-User data).<br>• Outage, significant slowdown, etc. (caused by failures related to the Tools or otherwise within GSA's reasonable control) which materially impacts or disables major functions from being performed and for which **no workaround is available.** |
| **Severity Two:** | **Business Defect with Workaround**<br>• Any problem that impacts the user's ability to use a major feature or function included in the Tools or the Customized Pages but does not prevent all useful work from being performed or does not disable major functions.<br>• Minor End-User data quality issue<br>• Software defects that result in unrecoverable End-User data loss or corruption but for which **a work around exists**. |
| **Severity Three** | **Non-material Error**<br>• Errors or non-conformity to specifications that have a minor impact on service performance.<br>• A defect that affects the user's ability to use minor features/functionality included in the Tools or the Customized Pages. |

| Reference Number | Severity One Incident Response Rules |
|---|---|
| 4.9.12 | For severity one incidents, GSA and effected Federation Members will make best efforts to provide telephone acknowledgement of report of error, or problem, within 15 minutes (or as promptly as possible thereafter), provided that such telephone acknowledgement shall in all cases be provided within 30 minutes. Incident updates should provided on an hourly basis. |
| 4.9.13 | For severity one incidents, Federation Members and GSA will assign dedicated resources immediately and continually work the problem until it is resolved. |

| Reference Number | Severity Two Incident Response Rules |
|---|---|
| 4.9.14 | For severity two incidents, Federation Members and GSA will provide telephone acknowledgement of report of error, or problem, within 60 minutes. Incident updates will be provided every two hours. |
| 4.9.15 | For severity two incidents, Federation Members and GSA determine a problem correction plan by the end of next business day. |

| Reference Number | Severity Three Incident Response Rules |
|---|---|
| 4.9.16 | For severity three incidents, Federation Members and GSA will provide telephone or email acknowledgement of report of error or problem within 24 hours. Incident updates will be provided on a daily basis. |
| 4.9.17 | For severity three incidents, Federation Members and GSA will determine a problem correction plan within five (5) business days. |

## 4.10 Metadata

Metadata will be shared between Federation Members. The following Rules apply:

| Reference Number | Metadata |
|---|---|
| 4.10.1 | Federation Members must make all Metadata[9] available to GSA who will share it with Connected Members and configure the Portal accordingly. |
| 4.10.2 | Federation Members must notify GSA of any planned Metadata changes no less than 6 weeks in advance of the changes. |
| 4.10.3 | Federation Members must respond to changes in other Federation Members' Metadata within 45 days of notification by GSA. |
| 4.10.4 | Federation Members must confirm receipt of Metadata change notices upon receipt. |
| 4.10.5 | GSA shall determine, issue, publish, and track AAID and CSID values as defined in the Technical Suite. |
| 4.10.6 | GSA shall maintain an up to date record of Federation Metadata and provide relevant excerpts to Federation Members as appropriate. |

## 4.11 Configuration Management

The following Configuration Management Rules apply:

| Reference Number | System Changes |
|---|---|
| 4.11.1 | GSA must be notified in advance of any substantial changes that affect other Federation Member Systems. |

| Reference Number | Change Management |
|---|---|
| 4.11.2 | Federation Members must comply with Federation Change Management Policy (see Appendix F). |
| 4.11.3 | Assertion-based CSs must establish a SAML connection with new Compatible RPs of the Federation within 90 days of the new Federation Member completing the Federation Boarding Process. CSs may delay these new connections so that no more than three (3) new RP connections are established in any given 90 day period. |
| 4.11.4 | Assertion-based RPs must establish a SAML connection with new Compatible CSs in the Federation within 90 days of the new Federation Member completing the Federation Boarding Process. Assertion-based RPs may delay these new connections so that no more than three (3) new CS connections are established in any given 90 day period. |
| 4.11.5 | GSA will publish Federation Member candidate status, including expected boarding completion date and Federation Member compatibility[10]. |

## 4.12 Optional Attributes

The technical suite references some attributes of the assertion that are optional. The following Rules apply:

| Reference Number | Optional Attributes |
|---|---|
| 4.12.1 | Assertion-based Federation Members may elect not to receive optional attributes. |
| 4.12.2 | Assertion-based RPs must notify GSA if any restrictions on optional attributes exist before going live. |
| 4.12.3 | Before going live, CSs sending SAML Assertions must notify GSA of which attributes they are willing and able to assert. |
| 4.12.4 | CSs sending SAML Assertions must not send attributes that RPs are prohibited from receiving. |
| 4.12.5 | GSA shall maintain records of the capabilities and restrictions related to optional attributes in the Federation.<br>1. These capabilities and restrictions must be incorporated into rollout planning as new Federation Members join the Federation.<br>2. GSA will notify Federation Members of these capabilities and restrictions for all Connected Members. |
| 4.12.6 | Federation Members must notify GSA in the event of any changes in capabilities or restrictions. |

## 4.13 Add-on Services

The technical suite provides a mechanism for additional services to be added to the trust relationship established between Federation Members[11]. The following Rules apply for any of these additional services:

| Reference Number | Requirement |
|---|---|
| 4.13.1 | Federation Members must notify GSA of the existence and nature of these services. |
| 4.13.2 | GSA will assist in the issuance of the service specification throughout the Federation if desired by the Federation Members. If requested by Federation Members, GSA will document the technical specification of how add-ons operate as part of the framework. Specifications will include explanations of data used in add-on services. |
| 4.13.3 | Add-on services are considered equal in their treatment of the E-Authentication architecture and Operating Rules. They will also adhere to the same laws and policies governing the architecture. |
| 4.13.4 | Add-on services will not require a separate agreement between a CSP/Letter of Designation (LoD) and the RP. |

## 4.14 Time Synchronization

For security and operational purposes, it is important that each Federation System have time synchronization. The following Rules apply:

| Reference Number | Requirement |
|---|---|
| 4.14.1 | Federation Member Systems must run time synchronization software such using NIST or Global Positioning Systems (GPS) servers. |

## 4.15 End-User Service

The following End-User service Rules apply:

| Reference Number | Requirement |
|---|---|
| 4.15.1 | Federation Members must make customer service contact information available to GSA. |
| 4.15.2 | Federation Members are entitled to use standardized customer service materials provided by GSA. |
| 4.15.3 | GSA shall provide telephone support from 8:00 a.m. to 8:00 p.m. (ET) to assist in identifying and resolving service problems and in answering questions related to the operational use of the services. |
| 4.15.4 | GSA shall make technical support personnel available from Monday through Friday 6:00 a.m. to 9:00 p.m. (ET) to assist identifying and resolving problems. |
| 4.15.5 | GSA shall provide emergency support on a 24x7 basis to solve problems which render the Federation inoperable to users or impair their functionality significantly (See Section 4.9 for Severity Levels). |
| 4.15.6 | As part of emergency support, GSA shall provide, and update, as needed, a list of individuals to be paged in resolution of such emergencies. |

## 4.16 Points of Contact

As mentioned in an earlier section of the Rules, communication is a key element to the operation of the Federation. As such, the following Rules apply:

| Reference Number | Requirement |
|---|---|
| 4.16.1 | All Federation Members must establish a principal point of contact (PPOC) for Federation communications that is available during their normal business hours. Alternatives must be established during vacation or travel. |
| 4.16.2 | The PPOC must be reachable during their normal business hours. |
| 4.16.3 | Each Federation Member must provide contact information for 2 secondary points of contact (SPOC) in the event the PPOC cannot be reached. |
| 4.16.4 | The PPOC and SPOC must be able to reach policy, technical, security, and operational representatives for their organization as needed to meet the requirements of these Rules. |
| 4.16.5 | GSA shall maintain a contact list with these point of contacts (POCs) and facilitate coordination and collaboration as needed and appropriate. |
| 4.16.6 | Each Federation Member must provide information on customer service channels to GSA for use in End-User assistance. |
| 4.16.7 | GSA shall maintain a customer service contact list for Federation Members and provide relevant information to Federation Members. |
| 4.16.8 | Federation Members must have on-call personnel available after normal business hours that are capable of acting as PPOC for emergency situations. |
| 4.16.9 | GSA will maintain an email address that will allow Federation Members to submit reports. |

## 4.17 GSA Architecture Components

GSA shall provide the following in regard to architecture components:

| Reference Number | Requirement |
|---|---|
| 4.17.1 | GSA shall make available the Federation Portal as defined in the Technical Suite. |
| 4.17.2 | GSA shall make available a Governing Authority Certification Authority as defined in the Technical Suite. |
| 4.17.3 | GSA shall make available one (1) or more Step Down Translators (SDTs) as defined in the Technical Suite. |
| 4.17.4 | GSA shall make available facilities needed for interoperability testing, including product testing and Federation Member acceptance testing. |
| 4.17.5 | GSA shall make test portals available for Federation Member integration testing as needed. |
| 4.17.6 | GSA shall maintain technical interface specifications. |
| 4.17.7 | GSA will provide, either directly or via a third-party, physical support of the GSA Systems 24x7, including support of power, air conditioning, physical security, and physical changes to existing Systems. |

## 4.18 Document Management

The following document management Rules apply:

| Reference Number | Requirement |
|---|---|
| 4.18.1 | GSA shall establish positive document control on all documentation distributed to the Federation.<br>1. Each document will be assigned a configuration item number and a version number.<br>2. Any updates to those documents will trigger a notification to the user group. |

## 4.19 Authoritative Documents

The following documents, as amended from time-to-time, are included by reference and are considered authoritative:

| Reference Number | Requirement |
|---|---|
| 4.19.1 | The CAF Suite. |
| 4.19.2 | The Technical Suite. |

## 4.20 Official Waiver(s)

While it is mandatory that each Federation Member sign a Participation Agreement (CSP or RP) stating they will adhere to the requirements set forth in the Federation Business and Operating Rules, there may be times when a Federation Member will be unable to satisfy certain requirements due to technical or operational limitations. In the event that a Federation Member may need a waiver, the process for issuing the waiver will be governed by the following guidelines:

| Reference Number | Official Waiver(s) |
|---|---|
| 4.20.1 | Only the GSA Manager of the Federation can approve waivers. Any disputes will be resolved by the GSA Program Executive (PE) or the GSA Deputy Program Manager. In the event of disputes that cannot be resolved by the PE or Deputy, the "court of last resort" for wavier disputes will be a standing committee of the GSA Executive Steering Committee (ESC), populated by at least two representatives from Agencies that are Federation Members and in good standing with the Federation. |
| 4.20.2 | The GSA Manager of the Federation shall ensure that no waiver materially effects the security and operational Integrity of the Federation. In addition, there will be no permanent waivers. |
| 4.20.3 | Waivers and supporting material will be shared among connected Federation Members. |
| 4.20.4 | Applications for waivers must be submitted using the Waiver Request Form, which will be available from GSA. |

## APPENDIX A: GLOSSARY

| Term | Definition |
|---|---|
| Access Control | Mechanisms and policies that restrict access to computer resources and/or facilities. |
| Activation | Activation is the process of mapping information contained in either the SAML Assertion or the public key certificate with the Agency Application's own database of users. |
| Agency | A Government owned corporation, which is considered a RP or CSP in regard to the Federation. |
| Agency Application (AA) | E-Government applications that perform some business function online. If an E-Government application has multiple interfaces (e.g., administration and service application), each interface with distinct authentication requirements is considered a stand-alone AA. AAs manage all Business Transactions and all End-User authorization decisions. |
| Approved | Acceptance by the GSA to participate in the E-Authentication Federation, or other inclusion or use in the E-Authentication Federation. |
| Approved Credential | A Credential issued to an End-User by an Approved Credential Service of an Approved Credential Service Provider |
| Approved Credential Service Provider | A Credential Service Provider or authorized agent that has been Approved by the GSA to participate in the E-Authentication Federation. |
| Approved Party | An Approved Relying Party, Credential Service Provider, or authorized agent. |
| Approved Relying Party | A Relying Party or authorized agent that has been approved by the GSA to participate in the E-Authentication Federation. |
| Assurance Level | Level of trust, as defined by the OMB Guidance for E-Authentication. This guidance describes four identity authentication Assurance Levels for E-Government transactions. Each Assurance Level describes the Agency's degree of certainty that the user has presented an identifier (a Credential in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the *vetting process* used to establish the identity of the individual to whom the Credential was issued, and 2) the degree of confidence that the individual who uses the Credential is the individual to whom the Credential was issued. The four levels of assurance are:<br>Level 1: Little or no confidence in the asserted identity's validity.<br>Level 2: Some confidence in the asserted identity's validity.<br>Level 3: High confidence in the asserted identity's validity.<br>Level 4: Very high confidence in the asserted identity's validity. |

| Term | Definition |
|---|---|
| Authentication Service Component (ASC) | A federated architecture that leverages Credentials from multiple domains through certifications, guidelines, standards adoption and policies. The ASC accommodates assertion-based authentication (i.e., authentication of PINs and Passwords) and certificate-based authentication (i.e., public key certificates) within the same environment. Over time, the architecture will leverage multiple emerging schemes such as the SAML and Liberty Alliance, and will not be built around a single scheme or commercial product. In this light, the ASC is more precisely defined as an architectural framework. |
| Authorization To Operate | Occurs when management authorizes a System based on an assessment of management, operational and technical controls. By authorizing processing in a System the management official accepts the Risk associated with it. |
| Availability | State of usability and functionality to provide operational effectiveness. |
| Binding Documents | E-Authentication Federation documents, in addition to the Participation Agreements, Business Rules and Operating Rules, that RPs and CSPs are required to adhere to and comply with. |
| Boarding Process | Includes all the activities involved in converting a Federation member candidate into an official Federation member. It includes an assessment to verify all applicable agreements and rules have been complied with (or waived), acceptance testing to ensure interface specification compliance, change control board (CCB) approval of member system integration, and CCB recommendation of the member candidate's request for a production E-GCA certificate. |
| Business Transaction | Business Transaction refers to the functionality of an Agency Application that was the basis of that applications Risk Assessment. |
| Business Rules | Core E-Authentication Federation principles (i.e., interoperability, auditing, and privacy) that RPs and CSPs must comply with. |

| Term | Definition |
|---|---|
| Certification and Accreditation (C&A) | Security Certification and Accreditation are important activities that support a Risk management process and are an integral part of an Agency's information security program.<br><br>Security accreditation is the official management decision given by a senior Agency official to authorize operation of an information System and to explicitly accept the Risk to Agency operations, Agency assets, or individuals based on the implementation of an agreed-upon set of security controls. Required by OMB Circular A-130, Appendix III, security accreditation provides a form of quality control and challenges managers and technical staffs at all levels to implement the most effective security controls possible in an information System, given mission requirements, technical constraints, operational constraints, and cost/schedule constraints. By accrediting an information System, an Agency official accepts responsibility for the security of the System and is fully accountable for any adverse impacts to the Agency if a breach of security occurs. Thus, responsibility and accountability are core principals that characterize security accreditation. |
| Chain of Custody | A set of procedure(s)/document(s) to account for the Integrity of an object by tracking its handling and storage from point of instantiation through the current or final disposition of the object. |
| Compatible | Two Federation Members are considered Compatible if:<br>1. the CS has an equal or higher Assurance Level than the RP,<br>2. the CS is willing and able to provide all optional attributes required by the RP,<br>3. and the Federation Members are currently using the same interface specification version. |
| Confidentiality | System and data Confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization. |
| Configuration Management (CM) | CM is conducted using the two interrelated functions:<br>• Configuration control<br>• Baseline management<br><br>Configuration control addresses CM policy and procedures, while baseline management is used to record changes over the life cycle. |

| Term | Definition |
|---|---|
| Connected Members | Connected Members are Federation Members that have directly connected their Systems to allow SAML exchanges. Every Member of the Federation is not connected to every other Federation Member, for example CSs are not connected to other CSs, higher Risk AAs are not connected to lower assurance CSs, etc. |
| Contractor | Person or entity that is under contract to provide the Federal Government with services, supplies, or other needs. |
| Credential | Digital documents used in authentication that bind an identity or an attribute to a subscriber's Token. Note that this document uses "Credential" broadly, referring to both electronic Credentials and Tokens. |
| Credential Service (CS) | System that authenticates an End-User who has a PIN or Password based identity Credential. The Credential Service then issues an identity assertion to the relying party. A Credential Service is a Verifier. |
| Credential Service Provider (CSP) | An organization that offers one or more Approved Credential Services. |
| Cryptography | The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31] Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2] |
| Data Integrity | The property that data has not been altered by an unauthorized entity. |
| E-Authentication Federation (Federation) | An identity federation, whereby Government agencies can rely on Credentials issued and managed by other organizations – within and outside the Federal Government. The Federation is driven by supply and demand. The demand is for online services, which will be fulfilled by leveraging an existing supply of trusted Credentials that are already available and in use by the American public. The Federation includes policy and standards, Business Rules, an architectural framework, Credential Services, Agency Applications, service delivery and acquisition, and a financial model. |
| E-Governance Certificate Authority (E-GCA) | Established by the Government to issue certificates that allow Agency Applications to retrieve SAML Assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate. |

| Term | Definition |
|---|---|
| Electronic Risk and Requirements Assessment, or E-RA (E-RA) | A risk-based approach to authentication requirements. This approach identifies the Risks associated with insufficient authentication of users, and it forms the basis for the definition of authentication requirements. |
| End-User | Any citizen, Government employee, contractor, or business that authenticates to an AA using a Credential issued by a CS. |
| Federation Change Management | Policies and processes agreed to by Federation Members to review, approve, and roll out architecture changes to production. |
| Federation Member | A Relying Party or Credential Service Provider that has successfully completed the preparation phase and the boarding phase. A Federation Member's System (Agency Application or Credential Service) is integrated into the production Authentication Service Component in the third and final phase of joining the Federation – the rollout phase. |
| Federation Operations Center | Organization within the PMO that operates and maintains the ASC production environment, and manages integration of Member Systems into the production ASC. |
| Federation Portal (Portal) | A website that helps End-Users locate the CSs and AAs they need to complete their transactions. The Portal also maintains information about CSs and AAs referred to as Metadata, which includes technical interface data as well as descriptive information. When the End-User opts into single sign-on, the Portal assigns a session cookie. |
| Federation Style Guide | Guidelines pertaining to Federation Member use of E-Authentication logos, branding, and providing E-Authentication instructions and information to End-Users via Federation Member System web pages. |
| Designated Financial Agent | Selected by a RP or CSP to provide financial related services in regard to the E-Authentication Federation. |
| Forensics | Process of gathering, processing, and interpreting digital and other evidence to conclusively solve a problem and/or derive a conclusion. |
| Hosted ASC Components | GSA Preferred hosting of ASC components. Unisys to host ASC components in the same facility, environment, and infrastructure. Each hosted component will be operated with the same direct management control. In addition, Unisys will support all hardware, operating Systems, and basic Network connectivity. Accordingly, Hosted ASC components are considered a single System. |
| Impact | The magnitude of harm that could be caused by a threat's exercise of a vulnerability. |

| Term | Definition |
|---|---|
| Informed Consent | Consent voluntarily signified by an End-User who is competent and who understands the terms of the consent and who has been provided in a clear statement with the appropriate knowledge needed to freely decide without the intervention of any element of force, fraud, deceit, duress, over-reaching or other ulterior form of constraint of coercion. Informed Consent may be signified by any method, including electronically, in a form or otherwise as provided by the party requesting the consent. |
| Integrity | Integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT System by either intentional or accidental acts. If the loss of System or Data Integrity is not corrected, continued use of the contaminated System or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of Integrity may be the first step in a successful attack against System Availability or Confidentiality. For all these reasons, loss of Integrity reduces the assurance of an IT System. |
| Log File | Audit trail of actions and/or exceptions. |
| Memo of Understanding | Executing an MOU begins the process of joining the E-Authentication Federation, and formally establishes an ongoing working relationship with the Initiative for an Agency. The MOU covers your commitments as an Agency, as well as the Initiative's commitment to your Agency. |
| Metadata | Information necessary for Nodes (Federation Member Systems) to technically interoperate. Metadata encompasses:<br><br>• E-Authentication specific information– scheme independent information pertaining to E-Authentication Federation Members (e.g., AA identifiers and CS identifiers) and E-Authentication policies (e.g., Assurance Levels, issuers, client/server certificates)<br>• Scheme specific information – information that directly supports technical interoperability for this scheme. Some or all of the Metadata for this scheme may not be used for a different E-Authentication scheme.<br><br>A Node must be configured with both E-Authentication specific Metadata and scheme specific Metadata. Failure to completely and correctly configure Metadata can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of Nodes. Metadata is not considered secret information. |

| Term | Definition |
|---|---|
| National Archives and Records Administration (NARA) | The National Archives and Records Administration Act of 1984 amended the records management statutes to divide records management responsibilities between the National Archives and Records Administration (NARA) and the General Services Administration (GSA). Under the Act, NARA is responsible for adequacy of documentation and records disposition and GSA is responsible for economy and efficiency in records management.<br><br>Section 3101 of title 44 U.S.C. requires the head of each Federal Agency to make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the Agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the Agency's activities. |
| Network | An open communications medium, typically the Internet, that is used to transport messages between the claimant and other parties. Unless otherwise stated no assumptions are made about the security of the Network; it is assumed to be open and subject to active (e.g., impersonation, man-in-the-middle, session hijacking…) and passive (e.g., eavesdropping) attack at any point between the parties (claimant, verifier, CSP or relying party). |
| Node | Synonym for "Federation Member System" in context of rolling out the System to or operating the System in the production Authentication Service Component (ASC) federated Network of interconnected Systems (Nodes). |
| Node Information Form | Form to be filled out by the Agency that documents essential information about the Agency's Node. Essential information includes Metadata values, assertion engine information, and E-GCA production certificate information. |
| Operating Rules | Day to day practices and policies Federation Members agree to in order to ensure Federation security, consistency, and service standards. |
| Operational Readiness Review | Federation Operations Center conducts an operational readiness review to determine whether the Federation member candidate's system is ready to be integrated into the production ASC. It includes final verification of the readiness of: Security, metadata, servers, node configuration, production scripts, capacity plans, escalation plans, Help desk, contact information, monitoring, training readiness, user support, documentation of testing, participation agreements, and production date coordination. |
| Participant | An End-User of the Federation. |

| Term | Definition |
|---|---|
| Password | A secret that a claimant memorizes and uses to authenticate his or her identity. Passwords are typically character strings. See also PIN. |
| Personal Identification Number (PIN) | A Password consisting only of decimal digits. |
| Personally Identifiable Information (PII) | Any information that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes information that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other Personally Identifiable Information can easily be derived, including, but not limited to, name, address, phone number, fax number, email address, financial profiles, and social security number, and credit card information. |
| Privacy Impact Assessment (PIA) | Privacy Impact Assessments are required by the E-Government Act of 2002 whenever "developing or procuring information technology . . . or initiating a new collection of information . . . in an identifiable form . . . ." The purpose of a Privacy Impact Assessment is to ensure there is no collection, storage, access, use or dissemination of identifiable personal information (and for some organizations business information) that is not both needed and permitted. |
| Program Management Office (PMO) | Established by the Government to issue certificates that allow Agency Applications to retrieve SAML Assertions from Credential Services over a client and server authenticated SSL channel, effectively controlling which entities can participate. |
| Public Key Certificate | A digital document issued and digitally signed by the private key of a Certification Authority that binds the name of a subscriber to a public key. The certificate indicates that the subscriber identified in the certificate has sole control and access to the private key. See also [RFC 3280]. |
| Relying Party | A Federal Agency that relies upon the End-User's Credentials, typically to process a transaction or grant access to information or a System. |
| Risk | Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization. |
| Risk Assessment | Risk Assessment is the first process in the Risk management methodology, used to determine the extent of the potential threat and the Risk associated with an IT System throughout its Software Development Life Cycle (SDLC). The output of this process helps to identify appropriate controls for reducing or eliminating Risk during the Risk mitigation process. |

| Term | Definition |
|---|---|
| Rule | A term or condition of participation manifested as an Operating Rule or Business Rule. |
| Rules of Behavior | Rules that have been established and implemented concerning use of, security in, and acceptable level of Risk for the System. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the System. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of System privileges, and individual accountability. |
| SAML Artifact | A SAML Artifact of "small" bounded size is carried as part of a URL query string such that, when the artifact is conveyed to the source site, the artifact unambiguously references an assertion. The artifact is conveyed via redirection to the destination site, which then acquires the referenced assertion by some further steps. Typically, this involves the use of a registered SAML protocol binding. This technique is used in the browser/artifact profile of SAML. |
| SAML Assertion | A statement from a verifier to a relying party that contains identity information about a subscriber. Assertions may also contain verified attributes. Assertions may be digitally signed objects or they may be obtained from a trusted source by a secure protocol. |
| Section 508 | In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. The purpose of this part is to implement Section 508 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794d). Section 508 requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, Federal employees with disabilities have access to and use of information and data that is comparable to the access and use by Federal employees who are not individuals with disabilities, unless an undue burden would be imposed on the Agency. Section 508 also requires that individuals with disabilities, who are members of the public seeking information or services from a Federal Agency, have access to and use of information and data that is comparable to that provided to the public who are not individuals with disabilities, unless an undue burden would be imposed on the Agency. |
| Security Assertion Markup Language (SAML) | XML-based framework for ensuring that transmitted communications are secure. SAML defines mechanisms to exchange authentication, authorization and nonrepudiation information, allowing single sign-on capabilities for Web services. |
| Sensitive Information | Information that must be protected due to the risk of loss or harm resulting from disclosure, alteration, or destruction. |

| Term | Definition |
|---|---|
| Service Level Agreement | Stipulates and commits a Federation Member to a required level of service. It also specifies, as appropriate, enforcement or penalty provisions for services not provided, a guaranteed level of System performance as relates to downtime or uptime, a specified level of customer support and what software or hardware will be used. |
| Session Identifier (SID) | Mechanism for indicating to the AA that there is prefill or data transfer available. |
| Session Reset | A request by an AA to re-authenticate an End-User already authenticated, resulting in a hand-off of the End-User to the CS. This request derives from the AA's Agency session policy. |
| Signatory | An Approved Party and the GSA who signs and is bound by the terms and conditions of this document. |
| System | System is a generic term used for briefness to mean either a major application or a general support System. |
| System of Records Notice | The Privacy Act of 1974 (5 U.S.C. § 552a, the Act) requires agencies to inform the public of the existence of Systems of Records containing personal information, to give individuals access to records about themselves in a System of Records, and to manage those records in a way to ensure fairness to individuals in Agency programs.<br><br>For the Privacy Act to work effectively, it is imperative that each Agency properly maintain its Systems of Records and ensure that the public is adequately informed about the Systems of Records the Agency maintains and the uses that are being made of the records in those Systems. Therefore, agencies must periodically review their Systems of Records and the published notices that describe them to ensure that they are accurate and complete. OMB Circular A-130, "Management of Federal Information Resources," (61 Fed. Reg. 6428, Feb. 20, 1996) requires agencies to conduct periodic reviews, and this memorandum satisfies that requirement for calendar year FY 1999. Agencies should continue to conduct reviews in accordance with the schedule in Appendix I of the Circular. |
| The Approved Technology Provider List | A list of software products that have demonstrated basic interoperability in the E-Authentication Interoperability Lab and are approved by the E-Authentication Initiative for use in the Federation. |
| Token | Something that the claimant (End-User) possesses and controls (typically a key or Password) used to authenticate the claimant's identity. |

| Term | Definition |
|---|---|
| Transaction Identifier (TID) | Mechanism for tracking transactions across various components in the architecture. TIDs will be generated by the Portal, and will be passed with the End-User, via query string, as they are redirected from (1) the Portal to CSs, (2) from CSs to AAs, and, (3) once generated by the Portal, to the Portal by AAs or CSs. TID is expected in Architecture 1.1. |
| Trust List | List of Certification Authorities that an application trusts. |

## APPENDIX B: ACRONYMS

| Acronym | Definition |
|---|---|
| AA | Agency Application |
| AAID | Agency Application Identifier |
| ASC | Authentication Service Component |
| CAF | Credential Assessment Framework |
| CMWG | Configuration Management Working Group |
| CS | Credential Service |
| CSID | Credential Service Identifier |
| CSP | Credential Service Provider |
| DNS | Domain Name System |
| DOS | Denial of Service |
| E-GCA | E-Governance Certificate Authority |
| E-RA | Electronic Risk and Requirements Assessment |
| ESC | Executive Steering Committee |
| ET | Eastern Time |
| FAQ | Frequently Asked Question |
| FCMP | Federation Change Management Policies |
| FISMA | Federation Information Security Management Act |
| FOC | Federal Operations Center |
| GMT | Greenwich Mean Time |
| GPS | Global Positioning System |
| GSA | General Services Administration |
| ID | Identifier |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| LoD | Letter of Designation |
| NIST | National Institute of Science and Technology |
| OMB | Office of Management and Budget |
| PII | Personally Identifiable Information |
| PIN | Personal Identification Number |
| PMO | Program Management Office |
| POC | Point of Contact |
| PPOC | Principle Point of Contact |
| PE | Program Executive |
| RP | Relying Party |

| Acronym | Definition |
|---|---|
| SAML | Security Assertion Markup Language |
| SID | Session Identifier |
| S/MIME | Secure/Multipurpose Internet Mail Extension |
| SPOC | Secondary Points of Contact |
| SDT | Step Down Translator |
| TBD | To Be Determined |
| TID | Transaction Identifier |
| UID | End-User Identifier |
| URL | Uniform Resource Locator |
| XML | Extensible Markup Language |

## APPENDIX C: MONITORING TEST TYPES

| Test Type | Frequency | Components Evaluated | Data Returned |
|---|---|---|---|
| Benchmark Test | 12 times per hour | Full HTML/No images | DNS, Connect, Redirect, 1st Byte, Content, Response Time |
| Transactional Test | 12 times per hour | Full HTML/No images/ per page data | DNS, Connect, Redirect, 1st Byte, Content, Response Time |
| Transactional Test | 4 times per hour | Full HTML/No images/ per page data | DNS, Connect, Redirect, 1st Byte, Content, Response Time |
| Full Page Download | 1 time per hour | Full HTML/Images | DNS, Connect, Redirect, 1st Byte, Content, Response Time |

**Note:** Response Time (RT) equals DNS + Connect + Redirect + 1st Byte + Content

# APPENDIX D: PERFORMANCE TESTING

## Availability Testing Criteria

This test is designed to verify the reliability and Availability of the service provided by Federation Members. Testing is limited to those services that are part of the Federation. Availability and data quality is considered in this test. Overall response time is not considered during this test, unless the Availability threshold is exceeded. This test will be measured from external locations.

| **Definition** | **Default Threshold** |
|---|---|
| Threshold Response Time | 60 seconds |
| Periodic Availability Threshold (based on three external monitoring locations - two out of three must pass tests) | 66.00% |
| Monthly Availability Threshold | 99.00% |

The Availability Test will be calculated as follows:

- The response time for each test in a five-minute window will be recorded for each test location.
- The response times for each test location within a five-minute window will then be evaluated versus the Threshold Response Time to determine which tests passed or failed. If Test Response Time is less than Threshold Response Time then the test passes, if not, the test fails.
- Based on the pass/fail status of each test location in a given window, a Periodic Pass Percentage will be calculated. (Number of Locations Passed / Total Number of Test Locations = Periodic Pass Percentage)
- The Periodic Pass Percentage will then be compared to the Periodic Availability Threshold to determine if the window is a Pass or a Fail. (If Periodic Pass Percentage is greater than Periodic Availability Threshold then the window passes, if not it fails)
- A Monthly Pass Percentage will be calculated based on the pass/fail status of all the windows in a given month. (Monthly Pass Percentage = Number of Window passes / Number of Windows for the Month)
- The Monthly Pass Percentage will then be compared to the Monthly Availability Threshold to determine if FOC passes or fails the test for the month. (If Monthly Pass Percentage is greater than or equal to the Monthly Availability Threshold then the month passes, if not it fails) If measurements made by CSP and FOC differ on whether a month has passed, CSP and FOC will work jointly to

determine whether the month has passed in accordance with the criteria set forth herein.

## Average Response Time

### *Testing*

This test is designed to ensure the service provided by Federation Members is, on average, delivered to the customer in a timely manner. Average response time, Availability and data quality are considered in this test. Tests will be measured over high-speed lines using a monitor that emulates the default behavior of the then-current version of Microsoft Internet Explorer. .

| **Definition** | **Default Threshold** |
|---|---|
| Monthly Average Response Time Threshold | 5 seconds |

The Average Response Time Test will be calculated as follows:

- The total response time for each test in a five-minute window will be recorded for each test location. If there are multiple web pages in the test, the total response time for all pages will be divided by the number of pages in the test to calculate the Average Page Response time for each location.
- The Average Page Response Times for each test location within a five-minute window will then be averaged to calculate the Periodic Average Response Time. This process will be repeated for every given window throughout the month.
- The Periodic Average Response Times will be averaged together to calculate the Monthly Average Time Response Time.
- The Monthly Average Time will then be compared to the Monthly Average Response Time Threshold to determine if the Federation Member passes or fails the test for the month. (If the Monthly Average Response Time is less than or equal to the Monthly Average Response Time Threshold then the month passes, if not it fails)

## Minimal Acceptable Response Time

### *Testing*

This test is designed to ensure the service provided by the Federation Member is delivered to the customer in a timely manner. Response time, Availability and data quality are considered in this test. Average response time is not considered during this test. Tests will be measured over high-speed lines using a monitor that emulates the default behavior of the then-current version of Microsoft Internet Explorer.

| **Definition** | **Default Threshold** |
|---|---|
| Threshold Response Time | 10 seconds |
| Periodic Minimum Acceptable Response Time Threshold (based on three external monitoring locations - two out of three must pass tests) | 66.00% |
| Monthly Minimum Acceptable Response Time Threshold | 99.00% |

The Minimum Acceptable Response Time Test will be calculated as follows

- The total response time for each test in a five-minute window will be recorded for each test location. If there are multiple web pages in the test, the total response time will be divided by the number of pages in the test to calculate the Average Page Response time for each location.
- The Average Page Response Times for each test location within a five-minute window will then be evaluated versus the Threshold Response Time to determine which tests passed or failed. (If Average Page Response Time is less than Threshold Response Time then the test passes, if not it fails)
- Based on the pass/fail status of each test location in a given window, a Periodic Pass Percentage will be calculated. (Number of Locations Passed / Total Number of Tests in a Window = Periodic Pass Percentage)
- The Periodic Pass Percentage will then be compared to the Periodic Minimum Acceptable Response Time Threshold to determine if the window is a Pass or a Fail. (If the Periodic Pass Percentage is greater than the Periodic Minimum Acceptable Response Time Threshold, then the window passes, if not it fails)
- A Monthly Pass Percentage will be calculated based on the pass/fail status of all the windows in a given month. (Monthly Pass Percentage = Number of Window passes / Number of Windows in the Month)
- The Monthly Pass Percentage will then be compared to the Monthly Minimum Acceptable Response Time Threshold to determine if the Federation Member passes or fails the test for the month. (If Monthly Pass Percentage is greater than or equal to the Monthly Minimum Acceptable Response Time Threshold then the month passes, if not it fails.

## Measurements

### *Availability Test*

| URL or object to be monitored | Test Type | Monitoring Frequency | Threshold Response Time | Periodic Availability Threshold | Monthly Availability Threshold |
|---|---|---|---|---|---|
| | Benchmark | 12 per hour | 60 seconds | 66.00% | **99.00%** |
| | Transactional | 12 per hour | | | |
| | Full Page Download | 1 per hour | | | |

### *Average Response Time Test*

| URL or object to be monitored | Test Type | Monitoring Frequency | Monthly Average Response Time Threshold |
|---|---|---|---|
| | Benchmark | 12 per hour | 5 seconds |
| | Transactional | 12 per hour | |
| | Full Page Download | 1 per hour | |

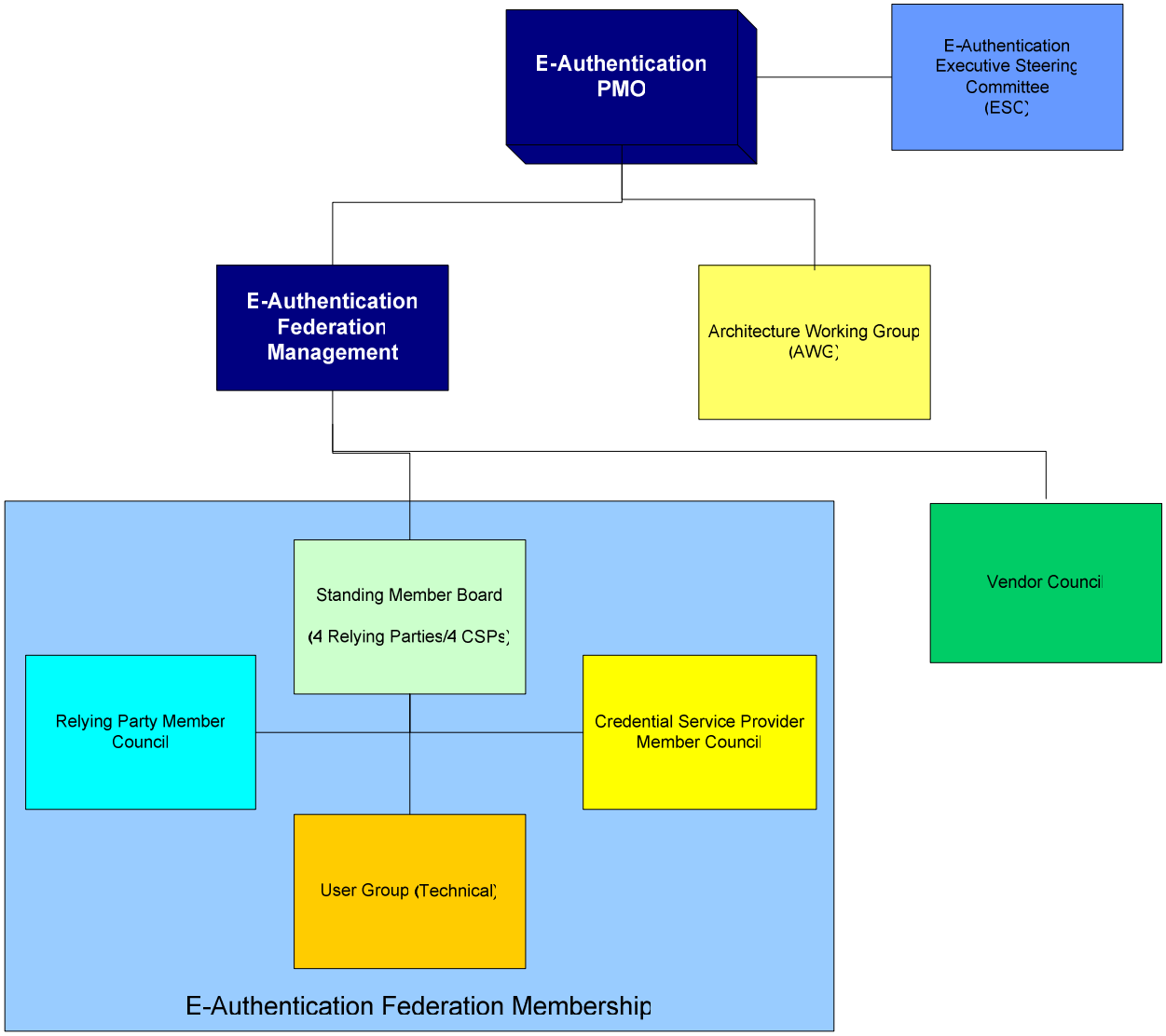
### *Minimal Acceptable Response Time Test*

| URL or object to be monitored | Test Type | Monitoring Frequency | Threshold Response Time | Periodic Minimum Acceptable Response Time Threshold | Monthly Minimum Acceptable Response Time Threshold |
|---|---|---|---|---|---|
| | Benchmark | 12 per hour | 10 seconds | 66.00% | **99.00%** |
| | Transactional | 12 per hour | | | |
| | Full Page Download | 1 per hour | | | |

## APPENDIX E: FEDERATION GOVERNANCE

The governance structure for the E-Authentication Federation is shown in the drawing below and is defined in the table that follows. The table indicates the lead or chair for each governing entity, a definition of the entity's membership, the role of the entity, and its decision-making authority, if any.

**Federation Governance Structure**



## Federation Governing Entities

| Entity | Chair | Membership | Role | Decision-Making |
|---|---|---|---|---|
| **Executive Steering Committee (ESC)** | Elected ESC Member | Cabinet-level Agency CIOs or CIO designee | Advisory and oversight responsibility for the E-Authentication Initiative including guidance on strategy and approval of the Initiative's business, spend, and funding plans. | Majority vote |
| **Program Management Office (PMO)** | Appointed by GSA | Program Executive, Deputy PM, and staff | Responsible for Federation Management, Operations, Management of Products/Services, and Acquisition Services, plus Project Management functions such as communications, reporting, budget, change management, and architecture. Required to raise issues to the ESC when requested by the SMB. | Program Executive |
| **Federation Management** | Deputy PM | Staff | Responsible for day to day Federation management and administration, outreach and recruitment of commercial CSPs and strategic E-Gov applications, relationship management of relying parties and CSPs, maintenance of the Business and Operating Rules and associated Federation documents, formation and management of Federation boards/groups/councils, change management, ensuring ongoing security and privacy of the Federation Network, and Federation membership compliance. | Deputy PM |
| **Standing Member Board (SMB)** | Elected by the membership, to rotate between a CSP and an RP | Four CSP representatives and four RP representatives, to include representation form both PKI and SAML relying parties, PKI and SAML CSPs, and gov't and commercial CSPs | Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management regarding issues that impact Federation membership. This Board will solicit input from the CSP Member Council, the RP Member Council, and the Federation User Group, as appropriate, and then will analyze, assess and compile recommendations to Federation Management. | Provides recommendations to Federation Management and the PMO, and can force the presentation of issues to the ESC. |
| **Credential Service Provider (CSP) Member** | Elected by the membership | One designated representative for each CSP Member of the Federation | Responsible for providing input and recommendations (either solicited or unsolicited) to the Standing Member Board regarding issues impacting CSPs including Federation Rules, E-Authentication architecture and | None. Provides input and recommendations to SMB on issues or changes. |

| | | | | |
|---|---|---|---|---|
| **Council** | | | technical specifications, current or potential schemes, the Credential Assessment Framework, the Federation membership System and other business and operations policies. Subcommittees may be created as necessary to address specific issues or proposed changes. | May present issues/concerns directly to Federation Management (PMO)<br>when deemed necessary/appropriate by Council membership. |
| **Relying Party (RP) Member Council** | Elected by the membership | One designated representative for each (RP) Member of the Federation | Responsible for providing input and recommendations (either solicited or unsolicited) to the Standing Member Board regarding issues impacting RPs including Federation Rules, E-Authentication architecture and technical specifications, current or potential schemes, the Relying Party Assessment Framework, the Federation membership System and other business and operations policies. Subcommittees may be created as necessary to address specific issues or proposed changes. | None. Provides input and recommendations to SMB on issues or changes.<br>May present issues/concerns directly to Federation Management (PMO)<br>when deemed necessary/appropriate by Council membership |
| **Vendor Council** | Appointed by the PMO | Representatives of vendors with Approved products within the E-Authentication architecture | Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management on issues impacting vendors and/or relative to commercial off-the-shelf electronic authentication products. | None. Provides input and recommendations to Federation Management |
| **Federation User Group** | Appointed by the Deputy PM | One or more representatives for each Member of the Federation | Responsible for providing input and recommendations (either solicited or unsolicited) to the Standing Member Board on issues impacting Federation Member users. Subcommittees may be created as necessary to address specific issues or proposed changes. | None. Provides input and recommendations to SMB on issues or changes |
| **Architecture Working Group** | E-Authentication Chief Architect (appointed by PMO) | Architectural subject matter experts (SMEs) recruited by the PMO | Responsible for making architectural and specification recommendations to the E-Authentication PMO at the request of the PMO or Chief Architect. | None. Provides input and recommendations to PMO relative to architectural issues and changes. |

## APPENDIX F: FEDERATION CHANGE MANAGEMENT POLICY

The purpose of this Appendix is to outline Federation Change Management Policies (FCMP). The PMO recognizes the need and importance of FCMP as part of the requirement for world-class operations. FCMP are complementary to the configuration or change management processes each Federation Member has established for itself.

FCMP is a framework within an overall Federation Change Management environment. FCMP is established to provide all Federation Members with:

1. Awareness and assurance that the Federation is operating appropriately,
2. Assurance that all changes are controlled, carefully reviewed and Approved, and
3. Assurance that Risks to service, reputation, and ongoing operations are identified, considered, and minimized.

The PMO has determined that the establishment of FCMP is critical. Therefore, the FCMP approach consists of several key steps to ensure consistency in communication, evaluation, and management, as well as to mitigate change-related Risks over time. This Appendix groups these steps into four major areas and addresses them in turn:

1. Change Classification
2. Change Evaluation
3. Approval
4. Compliance/Implementation

Each major area considers and/or is influenced by each change proposal profile. A change proposal profile is described in terms of four dimensions:

1. Category of change
2. Type of change
3. Impact of the change
4. Magnitude of the change

A change proposal profile influences required response times, change evaluation and approval time frames, and implementation and compliance time frames.

Change classification is considered the key initial step. It consists of determining the areas affected and magnitude. These decisions provide Federation Members with an evaluation frame of reference.

Change evaluation is the process by which the Federation's Standing Member Board (see Appendix E for a description of the Governance structure for the Federation), the Vendor Council, the Architecture Working Group (AWG), and other interested parties may assess the change according to the standard dimensions and to contribute feedback. Note that the Federation's Standing Member Board has the authority to leverage the Relying Party Member Council, the Credential Service Provider Member Council, and the Federation User Group (and its primarily technical membership) in order to obtain the appropriate level of analysis and input relative to potential changes. The change evaluation process and timeframes will be tailored appropriately according to the profile of the change in question. Changes bearing the same profile are expected to experience the same evaluation processes and timeframes.

Once a Federation change proposal is Approved, some or all Federation Members are required to implement the change. The timeframe to implement the change and to comply in the production environment is determined by the change proposal profile.

The final section of the document describes the change review process and the dispute resolution procedure.

## Change Classification

As described, a key component FCMP is change classification. Change classification results in a change proposal profile, which consists of several dimensions to capture the essence of the change. Once a change has been classified, the appropriate process for the change can be engaged.

The following classification dimensions are described below in further detail:

1. Category
2. Type
3. Impact
4. Magnitude

## Change Category

To be evaluated properly, changes must be categorized to provide guidance regarding Federation aspect(s) affected by the change. Understanding the affected aspect(s) allows Federation Members to evaluate the change in its correct context. It also allows Federation Members to better assess potential Impacts to the overall Federation and to individual Federation Members.

The following is a representative list of change categories:

1. Change in Federation membership
2. Update to Member System
3. Technical Specification changes
4. Scheme Introduction/Deprecation
5. Policies
6. Rules
7. Operational Requirements
8. ASC Component Changes

## Change Type

The degree of change will vary depending upon the type of change proposed. Describing the range of the anticipated change using consistent terms provides Federation Members necessary information regarding the extent of the change. The following table defines change types:

**Table 1: Change Types**

| **Change Types** | |
|---|---|
| Type | Description |
| *Evolutionary* | Evolutionary changes do not substantially alter the target of the change (e.g. clarifications). |
| *Revolutionary* | Revolutionary changes are anticipated to effect substantial change. |
| *Emergency* | Emergency changes are intended to address situations that place Federation Members in immediate jeopardy. These are of critical importance and extreme time sensitivity to Members of the Federation. |

## Impact

Impact refers to the breadth of the change with regards to the overall Federation, and is essential to evaluating proposed changes. The following table defines three levels of relative impact:

**Table 2: Impacts**

| **Impact** | |
|---|---|
| Level | Description |
| *Isolated* | Small pockets of the Federation are affected. |
| *Limited* | Less than half of Federation Members are affected. |
| *Broad* | Most of the Federation is likely to be impacted or affected by the change. |

## Magnitude

Regardless of type, scope, or category, all changes inherently require some cost. Magnitude is intended to provide a measure of the relative cost to Federation Members to implement a change, including direct costs and indirect costs related to activities or resources. As a single measure determined by the Federation Approved Parties, magnitude is not intended to divulge the precise cost estimates for individual organizations. The following table defines magnitudes:

**Table 3: Magnitudes**

| **Magnitude** | |
|---|---|
| Level | Description |
| *Low* | Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E). |
| *Medium* | Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E). |
| *High* | Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E). |

## Change Policies

Depending upon the change, rollout may consist of implementation or compliance. Rather than pre-define specific timeframes for implementation or compliance, the PMO recognizes that the period will depend heavily on the classification. Rollouts will be conducted by Federation Members and the PMO in accordance with the agreed-upon plan, as documented in the change proposal.

The E-Authentication architecture framework will be able to support multiple versions in order to account for varying life cycle needs, internal project management and prioritization and resource needs of Federation Members. The latest version of the architecture adopted will be downward compatible with prior versions supported. The earliest operating version of the architecture will be assigned a sunset date at which point it will no longer be supported. The sunset date will be 18-24 months after the implementation of the latest version. This will provide Federation Members ample lead time for the removal of a currently-supported version of the architecture. Emergency changes are not subject to the 18-24 month timeframe. However, it is expected that GSA's software development and quality assurance processes will ensure emergency changes introduced into the architecture framework will not adversely impact Federation Members.

## Release Rules

The following table defines release rules:

**Table 4: Release Rules**

| **Release Rules** | |
|---|---|
| Release | Description |
| *Emergency* | Emergency releases are done as needed. |
| *Minor* | Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E). |
| *Major* | Will be defined by Federation membership, consistent with Federation Governance Structure (Appendix E). |

## Change Management Policies

The basic FCMP policies are outlined based upon change type and category.

**Table 5: Policies for Change Types**

| **Policies for Change Types** | |
|---|---|
| **Evolutionary** | |
| | Evolutionary changes will occur no more than two times annually. |
| | The Standing Member Board will have at least 30 days to review and respond to proposed evolutionary changes. |
| | Official approval by appropriate Federation Approved Parties of finalized |

| | |
|---|---|
| | evolutionary changes will be submitted within 5 business days. |
| **Revolutionary** | |
| | Revolutionary changes should be rolled out no more than two times annually. |
| | The Standing Member Board will have at least 45 days to review and respond to proposed evolutionary changes |
| | Official approval by appropriate Federation Approved Parties of finalized revolutionary changes will be submitted within 10 business days. |
| **Emergency** | |
| | Emergency changes will be rolled out on an as needed basis to protect the Federation and its Members. |
| | The Standing Member Board will have at least 48 hours to review and respond to proposed emergency changes. |
| | Emergency changes will be implemented within 7 days of approval. |

## Policies for Change Categories

The following table defines policies related to change categories:

**Table 6: Policies for Change Categories**

| **Policies for Change Categories** | |
|---|---|
| **Change in Federation Membership** | |
| | New Federation Members must use Approved software or obtain a waiver. |
| | New Federation Members will be connected into the Federation incrementally. |
| | All new Federation Members must pass acceptance testing with the Interoperability Lab. |
| | Federation Member interaction must be confirmed by both parties before they are revealed by the Federation Portal. |
| **Update to Member System** | |
| | Updates to Federation Member Systems must be coordinated with the Federation Operations Center. |
| | Substantial changes to scheme implementation may require new acceptance testing. |
| | The Interoperability Lab will be made available to Federation Members for testing new releases upon request. |
| **Technical Specification Changes** | |
| | Substantial updates to the architecture will be vetted through the AWG. |
| | The Standing Member Board will have an opportunity to comment on proposed changes (30 days). |
| | The Vendor Council will have an opportunity to comment on proposed changes (30 days). |
| | All changes will include a rollout plan, provided to Federation Members for comments. |
| **Scheme Introduction/Deprecation** | |

| | |
|---|---|
| | New schemes will be adopted according to the policies/procedures in the technical approach. |
| | The rollout plan for scheme introduction or deprecation will follow the scheme adoption lifecycle as outlined in the *Technical Approach for the Authentication Service Component*. |
| | Federation Members will have at least 6 months notice before old schemes are abandoned. |
| **Policies** | |
| | The Standing Member Board will have 30 days to comment on proposed changes. |
| | Federation Members will have the time period to comply as determined during the change review process. |
| **Rules** | |
| | The Standing Member Board will have up to 30 days to review and comment. |
| | Federation Members have the time period to comply as determined during the change review process. |
| **Operational Requirements** | |
| | The Standing Member Board and the Vendor Council will have up to 30 days to review and comment. |
| | Federation Members have the time period to comply as determined during the change review process. |
| **ASC Component Changes** | |
| | The FOC will advise Federation Members of planned changes and provide a release plan. |
| | Changes to ASC components will follow the same guidelines as other Federation changes. |
| | The FOC will coordinate changes to ASC components with the user group. |

### Change Review and Implementation Process

Changes may originate from any source, but must be sponsored by either GSA, OMB, or a Federation Member to be considered. Changes are first submitted to the PMO. The PMO will then provide the change to the AWG and/or to Federation Management. For those changes assigned to Federation Management, Federation Management will review the changes, and as appropriate, provide them to the Standing Member Board for analysis and consideration by the CSP Council, the RP Council, and/or the Federation User Group. The Standing Member Board will then assess and compile resulting recommendations regarding the change and provide them to Federation Management, which will in turn provide them to the PMO. Recommendations regarding changes initiated or assessed by the AWG will also be provided to the PMO.

Implementation of the changes will occur according to the timelines indicated as part of the policies defined in Table 6 above.

## End Notes

[1] See Appendix A for TID definition.
[2] See Appendix A for SAML Assertion definition.
[3] See Appendix A for Business Transaction definition.
[4] Additional information is available at http://www.usdoj.gov/criminal/cybercrime/eprocess.htm .
[5] Those that are trusted by the Federation are provided at http://www.cio.gov/eauthentication/TCSPlist.htm .
[6] Test account requirements are defined in the *E-Authentication Interface Specifications*.
[7] See Appendix A for Connected Members definition.
[8] Availability and response times are specified in Appendix D.
[9] Metadata elements are defined in the *E-Authentication Interface Specifications*.
[10] See Appendix A for Compatible definition.
[11] This is accomplished through the use of the session identifier (SID) field in the assertion.